jamk.fi

Linux servers exercises

Arttu Karhunen
n4924@student.jamk.fi

Exercise
Syksy 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Exercise 1

Arttu Karhunen
n4924@student.jamk.fi

Exercise
Syyskuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

1 Task 1

Question:

Install Virtualbox to you machine from https://www.virtualbox.org... and install the Linux!

Answer:

Downloaded virtualbox from https://www.virtualbox.org/wiki/Downloads and CentOS from https://centos.org/download/.

then installed CentOS to virtualbox according to this instruction https://linuxhint.com/install_centos8_virtualbox/

I had problems connecting the server to network because I was at Dynamo using eduroam network (with my own laptop). Eduroam network didn't allow me to ping to google.com. After some googling I figured to connect laptop to my mobilephones network and ping.

2 Task 2

Question:

Since you have some perfect Linux server VM without any "real" services such as apache, samba or so.. now its the most perfect time to clone your VM to a template that can be used. You can do this in several ways,1. Export from the virtualbox2. Direct clone of the VM1st approach is recommended. Idea behind this is that in case you break something heavily or we need another server later (just might happen), then its not necessary to go and install all the Linux again. Instead you can just launch a new VM from your exported VM. Please note also: when you clone the VM with

OpenSSH server installed, the server keeps its host key. Thus you really should regenerate new SSH server keys after new VM is deployed. Also remember that you just might hit situation where your VMs have same IP or MAC address or so.

Answer:

After first VM was created I exported .ova file to my desktop and then imported it to virtualbox with different MAC address.

After cloning i changed both machines network settings from NAT to bridge and got them a different IP addresses.

Then I created new SSH keys to both machines with command:

```
ssh-keygen -t ed25519
```

3 Task 3

Since management of Linux machines is most often done through SSH, we do that as well in this course.

1. Login to your 1st Linux machine via SSH.

I installed Putty to my desktop and connected it to my first Linux with its IP and port number 22.

2. Set up SSH keys so there is no need to type password (nor even username) when logging in

   I used Putty connection manager to connect to CentOS from my desktop.
   I configured auto login with this guide https://www.technlg.net/windows/putty-auto-login-ssh-keys/
   I used WinSCP to copy the ssh key to my desktop

3. Set up the sudo access right management so that you can use sudo instead of su.

   I used this command to add my user to sudoers

   Sudo usermod -aG wheel *username*

jamk.fi

Exercise 2

Arttu Karhunen
n4924@student.jamk.fi

Exercise
Syyskuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Goal: Apply better network setup and a firewallNeeded stuff: Your Linux VMNotes: Quite easy task.

4 Task 1

Question:

Set up static IP addressing to your Linux server. Explain in the documentation why servers should have static IP addressing.

Answer:

I set up my static IP addres with network manager with command:

```
nmcli con mod enp0s3 ipv4.method manual ipv4.addr
192.168.1.10/24 ipv4.g 192.168.1.1
```

Server IP address should be static because that's make it easier for customers to find your server via DNS. Also makes easier to work remotely with server.

5 TASK 2

Set up firewall to your Linux server. Remember that you should allow SSH connections to your server.

To set up firewall I used firewalld to add rules.

First allow the SSH with command:

```
firewall-cmd --add-service=ssh --permanent
```

then allowed the web traffic:

```
firewall-cmd --add-port=80/tcp -permanent
```

and:

```
firewall-cmd --add-port=443/tcp -permanent
```

then activate the rules by reloading firewall with:

```
firewall-cmd --reload
```

checked those rules from the firewall with:

6 TASK 3

Set up fail2ban or some equivalent to your Linux server. Now test that fail2ban works as expected.

I installed and set up fail2ban as shown in: https://www.cyberciti.biz/faq/how-to-protect-ssh-with-fail2ban-on-centos-8/.
I used my virtual CentOS machine via other virtual CentOS to install and configure the fail2ban.

Made the /etc/fail2ban/jail.local configuration file and ignored my own IP address from banning with:

```
Ignoreip =1270.0.1/8 :: 192.168.2.12
```

Also changed the ban time to 5 min. then restart the fail2ban service and disconnected the ssh connection.

To test the fail2ban I try to reconnect my virtual machines via ssh and gave the wrong password 3 times. After that the IP was banned and I couldn't try to connect it anymore.
Checked the fail2ban banned IP's and found 1 that was my other virtual CentOS machine.
In /var/fail2ban.log file founded 3 logging attempts and action to ban the IP.

jamk.fi

Exercise 3

The LAMP stack

Arttu Karhunen
n4924@student.jamk.fi

Exercise
Syyskuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Goal: Successfully install LAMP stack to your LinuxNeeded stuff: Your Linux VMNotes: This is far more difficult than previous task. Remember that your firewall might prevent something...

7 TASK 1

Question:

Install the LAMP stack to your Linux server. Try to search web for instructions with keywords e.g.“how to install lamp stack gentoo”

Answer:

Installed LAMP with these instructions: https://www.tecmint.com/install-lamp-on-centos-8/

I installed it to my CentOS 8 VM.

8 TASK 2

Question:

Set up so that your users can have their ~/public_html visible through the Apache. You can try it e.g. with index.html:<html><body>Hello world!</body></html>

Answer:

First I added virtualhost. Configured virtualhost to /etc/httpd/conf.d/ directory.

```
<VirtualHost *:80>
        ServerName firstpage.com
        DocumentRoot /var/www/html/
</VirtualHost>
```

Then added directory to /var/www/html directory and then added index.html files to them.

9 TASK 3

Question:

Set up another user account to your server and also public_html folder and some web page under that account.

Answer:

First create a new user and password to user with:

 # Useradd testuser1

 # passwd testuser1

For another user I created another virtualhost to same folder as previous. Then added users web page directory to /var/www/html directory and added html web page in that folder.

Then I changed the ownership of those web page folders:

```
$ sudo chown -R $USER:$USER /var/www/html/firstpage.com/public_html
```

jamk.fi

10 TASK 4

Question:

set up .htaccess to your own user home directory so that it requires username and password. Please use some non-legit username and password since we are probably going to capture those later in these exercises.

Answer:

First change AllowOverride from None To All in:

$ /etc/httpd/conf/httpd.conf

Next restart apache with:

$ sudo systemctl reload httpd

Then created .htaccess file to /var/www/html/firstpage.com/public_html

Then created folder and usernames and passwords with:

$ sudo htpasswd -c /etc/safe_location/.htpasswd username

And added password in that file

jamk.fi

Next edit .htaccess to enable authentication with:

AuthUserFile /etc/safe_location/.htpasswd

AuthGroup /dev/null

AuthName “Please Enter Password”

AuthType Basic

Require valid-user

jamk.fi

Exercise 4

Wordpress setup

Arttu Karhunen
n4924@student.jamk.fi

Exercise
Syyskuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Goal: Install wordpress to your LAMP server

Needed stuff: Your Linux VM with LAMP

Notes: Enjoy!TASK

11 TASK 1

Question:

Install wordpress to your Linux server. There is a great number of examples in the web regarding Wordpress installation. Use them, and please,add the source to your exercise document.

Answer:

Used this example to install wordpress: https://upcloud.com/community/tutorials/install-word-press-lemp-centos-8/

Already had LAMP stack so only made database and downloaded wordpress and configured it.

I had problems to download wordpress with wget because every time the file got corrupted. Then I Downloaded it to my other laptop and sent it with scp to my CentOS VM.

jamk.fi

Exercise 5

SELinux

Arttu Karhunen
n4924@student.jamk.fi

Exercise
Syyskuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Goal: SELinuxNeeded stuff: Your Linux VMNotes: Super effortless task, just

12 TASK 1

Question:

Check if your Linux VM has SELinux enabled. Then check its status and possible log files it uses. What information can you find out? If you have SELinux enabled, how is it treating your Apache?

Answer:

Check /etc/sysconfig/selinux

In file: SELINUX=enforcing ja SELINUXTYPE=targeted

OR

sestatus

SELinux log file is in: /var/log/audit/audit.log

Opened log files with sealaert:

Yum install setroubleshoot-server

Sealert -a /var/log/audit /audit.log

The log shows that SELinux is preventing httpd to accessing to network because httpd_can_network-connect is disabled.

13 TASK 2

Question:

Check if your Linux VM has Apparmor enabled. Then check its status and possible log files it uses. What information can you find out? If you have Apparmor enabled, how is it treating your Apache

Answer:

Cento 8 doesn’t have apparmor

jamk.fi

Exercise 6

Setting up HTTPS

Arttu Karhunen
n4924@student.jamk.fi

Exercise
Lokakuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Goal: Apply security

Needed stuff: Your Apache with word-press

Notes: This requires some setting up...

14 TASK 1

Question:

To verify that the usage of HTTP is bad, time to capture credentials! Install a wireshark to your machine and start to capture traffic between your machine and the Linux server with Wordpress. Then login to the wordpress admin page using your credentials. Stop the wireshark capture and find out the login credentials from there.

jamk.fi

Answer:

Authentication messages in wireshark:

15857	6731.713881	192.168.10.241	192.168.10.199	HTTP	702 HTTP/1.1 401 Unauthorized (text/html)
15875	6739.036430	192.168.10.199	192.168.10.241	HTTP	376 GET / HTTP/1.1

GET message opened where you can see Authorization basic message encrypted with base64, which is easy to decrypt and get the password and username.

```
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: en-US,en;q=0.7,fi;q=0.3
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: 192.168.10.241
Connection: Keep-Alive
Authorization: Basic [redacted]
```

jamk.fi

15 TASK 2

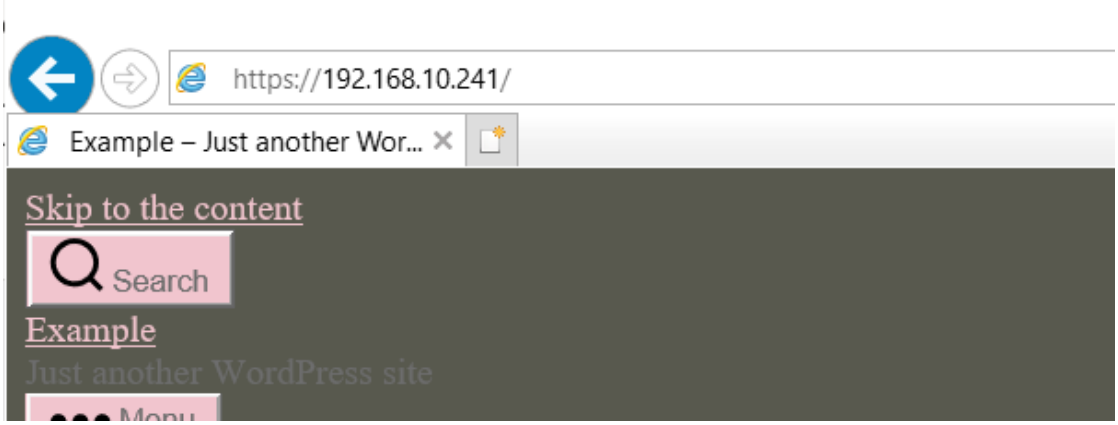
Question:

Enable HTTPS (TLS) on your Apache web server. Do this for instance with https://wiki.centos.org/HowTos/Https

Verify the TLS connectivity with e.g. wireshark or directly via browser.

Answer:

Browser don’t let open https pages with self-signed certificate. Explorer was able to open when changed settings to allow that also bitdefender warned about opening the page.



16 TASK 3

Question:

Since we have HTTP and HTTPS both now active, change the Apache settings so that the HTTP re-directs clients to use HTTPS. You can search this from the web e.g. “http to https redirect”

Answer:

Used this tutorial to redirect http to https:

https://www.digitalocean.com/community/tutorials/how-to-create-a-self-signed-ssl-certificate-for-apache-on-centos-8

Just need to set up a `VirtualHost` to respond to these unencrypted requests and redirect them to HTTPS by adding this to wordpress configuration file.

```
<VirtualHost *:80>
    ServerName 192.168.10.241
    Redirect / https://192.168.10.241
</VirtualHost>
```

17 TASK

Question:

Ok, what was the problem with the certificates in the TASK 2? Before proceeding, please check the certificate issuer and the common name using your favorite web browser. Add a screenshot containing the issuer and CN.

Answer:

First error was: PR_END_OF_FILE_ERROR. That was probaply because bitdefender was intercepting the connection and sent different certificate.

After disabling the bitdefender I got **SEC_ERROR_CA_CERT_INVALID** because I had non-authorized certificate:

jamk.fi

Kohteen nimi	
Maa	FI
Sijainti	JYVASKYLA
Organisaatio	Default Company Ltd
Yleinen nimi	arttu
Myöntäjän nimi	
Maa	FI
Sijainti	JYVASKYLA
Organisaatio	Default Company Ltd
Yleinen nimi	arttu

After that i changed my certificate CN to my IP:

Kohteen nimi	
Maa	FI
Sijainti	JKL
Organisaatio	Default Company Ltd
Yleinen nimi	192.168.10.241
Myöntäjän nimi	
Maa	FI
Sijainti	JKL
Organisaatio	Default Company Ltd
Yleinen nimi	192.168.10.241

Then I got MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT and firefox said that certificate is not trusted because it is self signed.

jamk.fi

Exercise 7

Linux monitoring

Arttu Karhunen
n4924@student.jamk.fi

Exercise
Lokakuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Goal: Understand the monitoring tools
Needed stuff: Your Linux VM
Notes: Quite easy task.

18 TASK 1

Question:

Check what information you can have from the machine using the top and iftop commands.

Answer:

top command is used to show the Linux processes. It provides a dynamic real-time view of the running system. Usually, this command shows the summary information of the system and the list of processes or threads which are currently managed by the Linux Kernel.

iftop command listens to network traffic on a named network interface, or on the first interface, it can find which looks like an external interface if none is specified, and displays a table of current bandwidth usage by pairs of hosts. The iftop is a perfect tool for remote Linux server over an ssh based session

19 TASK 2

Install sysstat package and learn how to use sar command. Especially learn how to generate reports for CPU and memory usage. Configure sar to collect data every 15 minutes. Nice guide for this: https://www.linuxtechi.com/generate-cpu-memory-io-report-sar-command/

Oh: no need to generate reports daily, instead generate reports by hand when necessary.

Answer:

Create sysstat file to /etc/cron.d and configure:

```
[arttu@centos cron.d]$ cat /etc/cron.d/sysstat
# Run system activity accountig tool every 15 minutes
*/15 * * * * root /usr/lib64/sa/sa 1 1
# 0 * * * * root /usr/lib64/sa/sa1 600 6 &
# Generate a daily summary of process accountig at 23.53
53 23 * * * root /usr/lib64/sa/sa2 -A
[arttu@centos cron.d]$
```

Disable reports in /etc/sysconfig/sysstat file:

```
# By default sa2 script generates reports files (the so called sarDD files).
# Set this variable to false to disable reports generation.
REPORTS=false
```

20 TASK 3

Start either bwm-ng and iotop, or even both to monitor your network interfaces for the next task.

Answer:

```
bwm-ng v0.6.2 (probing every 0.500s), press 'h' for help
input: /proc/net/dev type: rate
\         iface                   Rx                 Tx              Total
==============================================================================
         enp0s3:           0.00  B/s           0.00  B/s           0.00  B/s
            lo:           0.00  B/s           0.00  B/s           0.00  B/s
------------------------------------------------------------------------------
          total:           0.00  B/s           0.00  B/s           0.00  B/s
```

21 TASK 4

Install Netdata to your server. (https://github.com/netdata/netdata)Monitor the downloading part using software started in the previous task. After downloading is complete, you can close up these monitoring tools. Remember that Netdata collects “anonymous usage information” and sent to Google Analytics. There is nice way to stop this as explained: https://github.com/netdata/net-data/blob/master/docs/anonymous-statistics.md#opt-out

Answer:

Traffic from bwm-ng:

```
Inter-|   Receive                                                |  Transmit
 face |bytes    packets errs drop fifo frame compressed multicast|bytes    packets errs drop fifo c$
enp0s3: 9689825    7004    0    0    0     0          0         0   265580    3490    0    0    0  $
    lo:       0       0    0    0    0     0          0         0        0       0    0    0    0  $
```

Configuring netdata not to send anonymous statistics to netdata:

```
[arttu@centos netdata]$ sudo touch .opt-out-from-anonymous-statistics
[arttu@centos netdata]$ ls
conf.d  netdata.conf
[arttu@centos netdata]$ ls -la
total 20
drwxr-xr-x.  3 root root   82 Oct 18 19:58 .
drwxr-xr-x. 92 root root 8192 Oct 18 19:37 ..
drwxr-xr-x.  6 root root 4096 Oct 18 19:37 conf.d
-rw-r--r--.  1 root root  613 Oct 18 19:43 netdata.conf
-rw-r--r--.  1 root root    0 Oct 18 19:58 .opt-out-from-anonymous-statistics
[arttu@centos netdata]$
```

22 TASK 5

Time to load your server. You can try whatever way to load it, remember that some of them might need a lot of disk space. Sophisticated, and easy, way to give some load is to use openssl: openssl speed -multi 1the 1 parameter mean number of CPU cores. What resource that command loads/tests? Take (and insert to exercise document) a screenshot displaying the load in whatever tool you prefer

Answer:

jamk.fi

```
+R7:133582:253:10.00
+DTP:448::ecdh:10
+R7:10545:448:10.01
+DTP:253:sign:Ed25519:10
+R8:136157:253:Ed25519:10.01
+DTP:253:verify:Ed25519:10
+R9:52152:253:Ed25519:10.01
+DTP:456:sign:Ed448:10
+R8:17053:456:Ed448:10.01
+DTP:456:verify:Ed448:10
+R9:9811:456:Ed448:10.01
Got: +H:16:64:256:1024:8192:16384 from 0
Got: +F:0:md2:1952202.67:3861219.93:5160058.47:5691733.33:5854150.17:5851428.57 from 0
Got: +F:1:mdc2:0.00:0.00:0.00:0.00:0.00:0.00 from 0
Got: +F:2:md4:51803231.89:166722530.23:383648853.33:566187630.56:674402998.01:677453905.65 from 0
Got: +F:3:md5:77186245.33:175097961.46:303174591.36:378995667.77:402072582.78:393471829.90 from 0
Got: +F:4:hmac(md5):28171557.33:97974134.22:226648026.58:340914434.55:401754794.67:402257137.54 from
 0
Got: +F:5:sha1:77003184.00:182527786.67:322876555.48:430234110.30:499913398.01:509145047.18 from 0
Got: +F:6:rmd160:26667476.41:64091024.58:117654793.36:150122154.67:161110240.53:162577180.07 from 0
Got: +F:7:rc4:380190065.12:415924390.70:353903445.33:348177009.97:339600584.72:323320005.32 from 0
Got: +F:8:des cbc:44935552.00:46729962.67:46944701.66:46896818.60:47065770.67:46544712.29 from 0
Got: +F:9:des ede3:16910793.36:17632510.30:17540167.44:17656490.67:17608717.61:17619603.99 from 0
Got: +F:10:idea cbc:58057052.49:59329892.36:60636757.33:60564326.91:58623149.50:39038554.15 from 0
Got: +F:11:seed cbc:40878922.67:58723976.08:59803811.30:59451875.08:60254890.67:59902299.00 from 0
Got: +F:12:rc2 cbc:31121584.05:31364039.87:31353791.36:31817728.00:31643981.40:31728350.83 from 0
Got: +F:13:rc5-32/12 cbc:161571949.50:178703893.33:183155922.92:184996316.28:184736403.99:184762368.
00 from 0
Got: +F:14:blowfish cbc:76876483.17:81765802.67:84461544.19:86643327.57:87113728.00:86835200.00 from
 0
Got: +F:15:cast cbc:70982118.27:76344898.34:77996288.00:78023697.01:72892416.00:63460693.33 from 0
Got: +F:16:aes-128 cbc:80919473.75:90358293.33:93310384.05:213677161.46:203275906.98:181747712.00 fr
om 0
Got: +F:17:aes-192 cbc:61563253.16:74819146.84:76937610.63:177574867.77:181974357.33:180338306.98 fr
om 0
Got: +F:18:aes-256 cbc:59552512.00:64758878.41:63104853.33:153703080.40:155000260.47:153993270.43 fr
om 0
```

jamk.fi

```
Got: +F:5:sha1:77003184.00:182527786.67:322876555.48:430234110.30:499913398.01:509145047.18 from 0
Got: +F:6:rmd160:26667476.41:64091024.58:117654793.36:150122154.67:161110240.53:162577180.07 from 0
Got: +F:7:rc4:380190065.12:415924390.70:353903445.33:348177009.97:339600584.72:323320005.32 from 0
Got: +F:8:des cbc:44935552.00:46729962.67:46944701.66:46896818.60:47065770.67:46544712.29 from 0
Got: +F:9:des ede3:16910793.36:17632510.30:17540167.44:17656490.67:17608717.61:17619603.99 from 0
Got: +F:10:idea cbc:58057052.49:59329892.36:60636757.33:60564326.91:58623149.50:39038554.15 from 0
Got: +F:11:seed cbc:40878922.67:58723976.08:59803811.30:59451875.08:60254890.67:59902299.00 from 0
Got: +F:12:rc2 cbc:31121584.05:31364039.87:31353791.36:31817728.00:31643981.40:31728350.83 from 0
Got: +F:13:rc5-32/12 cbc:161571949.50:178703893.33:183155922.92:184996316.28:184736403.99:184762368.
00 from 0
Got: +F:14:blowfish cbc:76876483.17:81765802.67:84461544.19:86643327.57:87113728.00:86835200.00 from
 0
Got: +F:15:cast cbc:70982118.27:76344898.34:77996288.00:78023697.01:72892416.00:63460693.33 from 0
Got: +F:16:aes-128 cbc:80919473.75:90358293.33:93310384.05:213677161.46:203275906.98:181747712.00 fr
om 0
Got: +F:17:aes-192 cbc:61563253.16:74819146.84:76937610.63:177574867.77:181974357.33:180338306.98 fr
om 0
Got: +F:18:aes-256 cbc:59552512.00:64758878.41:63104853.33:153703080.40:155000260.47:153993270.43 fr
om 0
Got: +F:19:camellia-128 cbc:69402576.00:103101661.13:114388650.67:114912531.56:118751232.00:11710477
6.08 from 0
Got: +F:20:camellia-192 cbc:58737153.49:80050325.33:87869746.18:91176143.52:91668752.16:91527229.24
from 0
Got: +F:21:camellia-256 cbc:57712378.67:80634195.35:88281557.48:90749873.75:92474026.67:91881036.54
from 0
Got: +F:23:sha256:44043162.67:98032478.41:170113530.90:210705749.33:225247232.00:224662198.01 from 0
Got: +F:24:sha512:26751308.97:96736871.76:149608781.40:246720853.33:277333219.93:281826572.76 from 0
Got: +F:25:whirlpool:22698136.88:48985066.67:81781879.07:97634487.71:99803598.67:104802986.67 from 0
Got: +F:26:aes-128 ige:80960586.67:85604762.79:86436741.53:87090009.30:87570030.56:88326144.00 from
0
Got: +F:27:aes-192 ige:62898902.33:61073173.33:64455356.81:73543338.67:73151021.93:72448850.50 from
0
Got: +F:28:aes-256 ige:59604624.58:62382826.67:62620491.69:63091667.77:60541873.75:63168212.62 from
0
Got: +F:29:ghash:199163717.33:266995710.30:292283109.63:296294741.33:301400064.00:299344360.26 from
0
Got: +F:30:rand:3655221.19:13422037.33:40772295.02:83683593.36:119913461.79:125277525.33 from 0
```

jamk.fi

```
Got: +F:30:rand:3655221.19:13422037.33:40772295.02:83683593.36:119913461.79:125277525.33 from 0
Got: +F2:0:512:13660.239760:191884.800000 from 0
Got: +F2:1:1024:4850.349650:75506.900000 from 0
Got: +F2:2:2048:676.623377:22781.118881 from 0
Got: +F2:3:3072:208.491508:10036.063936 from 0
Got: +F2:4:4096:94.017946:5995.300000 from 0
Got: +F2:5:7680:11.000991:1765.734266 from 0
Got: +F2:6:15360:1.794616:431.168831 from 0
Got: +F3:0:512:8672.327672:14910.189810 from 0
Got: +F3:1:1024:4258.400000:5807.100000 from 0
Got: +F3:2:2048:1490.509491:1709.500000 from 0
Got: +F4:0:224:9661.600000:4260.500000 from 0
Got: +F4:1:256:21660.079840:7647.200000 from 0
Got: +F4:2:384:568.400000:694.211577 from 0
Got: +F4:3:521:1920.200000:981.900000 from 0
Got: +F5:0:224:6295.404595:0.000159 from 0
Got: +F5:1:256:10304.395604:0.000097 from 0
Got: +F5:2:384:587.900000:0.001701 from 0
Got: +F5:3:521:1594.610778:0.000627 from 0
Got: +F5:4:253:13358.200000:0.000075 from 0
Got: +F5:5:448:1053.446553:0.000949 from 0
Got: +F6:0:253:Ed25519:13602.097902:5209.990010 from 0
Got: +F6:1:456:Ed448:1703.596404:980.119880 from 0
OpenSSL 1.1.1c FIPS  28 May 2019
built on: Fri Apr 24 03:32:11 2020 UTC
options:bn(64,64) md2(char) rc4(16x,int) des(int) aes(partial) idea(int) blowfish(ptr)
compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -O3 -O2 -g -pipe -Wall -Werror=format-secu
rity -Wp,-D_FORTIFY_SOURCE=2 -Wp,-D_GLIBCXX_ASSERTIONS -fexceptions -fstack-protector-strong -grecor
d-gcc-switches -specs=/usr/lib/rpm/redhat/redhat-hardened-cc1 -specs=/usr/lib/rpm/redhat/redhat-anno
bin-cc1 -m64 -mtune=generic -fasynchronous-unwind-tables -fstack-clash-protection -fcf-protection -W
a,--noexecstack -Wa,--generate-missing-build-notes=yes -specs=/usr/lib/rpm/redhat/redhat-hardened-ld
 -DOPENSSL_USE_NODELETE -DL_ENDIAN -DOPENSSL_PIC -DOPENSSL_CPUID_OBJ -DOPENSSL_IA32_SSE2 -DOPENSSL_B
N_ASM_MONT -DOPENSSL_BN_ASM_MONT5 -DOPENSSL_BN_ASM_GF2m -DSHA1_ASM -DSHA256_ASM -DSHA512_ASM -DKECCA
K1600_ASM -DRC4_ASM -DMD5_ASM -DAES_ASM -DVPAES_ASM -DBSAES_ASM -DGHASH_ASM -DECP_NISTZ256_ASM -DX25
519_ASM -DPOLY1305_ASM -DZLIB -DNDEBUG -DPURIFY -DDEVRANDOM="\"/dev/urandom\"" -DSYSTEM_CIPHERS_FILE
="/etc/crypto-policies/back-ends/openssl.config"
[arttu@centos netdata]$
```

jamk.fi

Exercise 8

SAMBA

Arttu Karhunen
n4924@student.jamk.fi

Exercise
Lokakuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Goal: Create SAMBA fileshare
Needed stuff: Your Linux server and your own PC as client !
Notes: Things can get complicated, or not.

23 TASK 1

Question:

Install samba server to your Linux server

Answer:

To install Samba, we run:

```
sudo apt update
sudo apt install samba samba-client
```

We can check if the installation was successful by running:

```
whereis samba
```

The following should be its output:

```
samba: /usr/sbin/samba /usr/lib/samba /etc/samba /usr/share/samba
/usr/share/man/man7/samba.7.gz /usr/share/man/man8/samba.8.gz
```

---

jamk.fi

24 TASK 2

Question:

Configure the samba first in a way that user home folders are shared and can be accessed only by the corresponding user. Test this configuration using e.g. your own workstation. Verify also that users cannot access home folder of another user. What kind of configuration in /etc/samba/smb.conf holds for this step?

Answer:

Add to

The configuration file at /etc/samba/smb.conf. uncomment and change lines:
[homes]
comment = Home Directories
browseable = yes

Restart samba
```
Sudo service smbd restart
```
Allow at firewall:
```
Sudo ufw allow samba
```

Add user to samba:
```
Sudswd -a username
```

Change home directories ownership to the correct user:
```
# chown user:group /home/user
```

Then set permission to right user to access the home folder:
```
# chmod -R 0770 /home/user
```

Tested that each user can access to own home folder -> OK

jamk.fi

25 TASK 3

Question:

Make a new folder to your system. e.g. /srv/samba/openshare And make a new share to your samba configurations so that anybody has read and write access to that share. Whats the problem with this kind of share?
Answer:

Added these configurations to /etc/samba/smb.conf:

```
[openshare]
   comment = public shared folder
   path = /srv/samba/openshare
   browseable = yes
   writable = yes
   guest ok = yes
   create mask = 0660
   directory mask = 0770
   public = yes
```

Give permission to file:

 # sudo chmod 777 /srv/samba/openshare

Problem is that anyone can add anything to this file. There is no authentication who have inserted files to that directory.

jamk.fi

Exercise 9

Caching proxy server

Arttu Karhunen
n4924@student.jamk.fi

Exercise
Lokakuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Goal: Setup Proxy server
Needed stuff: Your Linux VM
Notes: Quite easy task.

26 TASK 1

Question:

Install squid proxy to your Linux server. Configure your browser to use that. Firefox will be the easiest one. Verify configuration. You should be able to do this by e.g. capturing data using tcpdump from the Linux server or monitoring the log files or the size of cache file location. Further make sure that your squid server acts as a caching server. Where are the cache files stored in your file system?

Answer:

Installing squid to ubuntu:

```
$ sudo apt -y install squid
$ sudo systemctl start squid
$ sudo systemctl enable squid
```

Squid configure file：

```
$ sudo nano /etc/squid/squid.conf
```

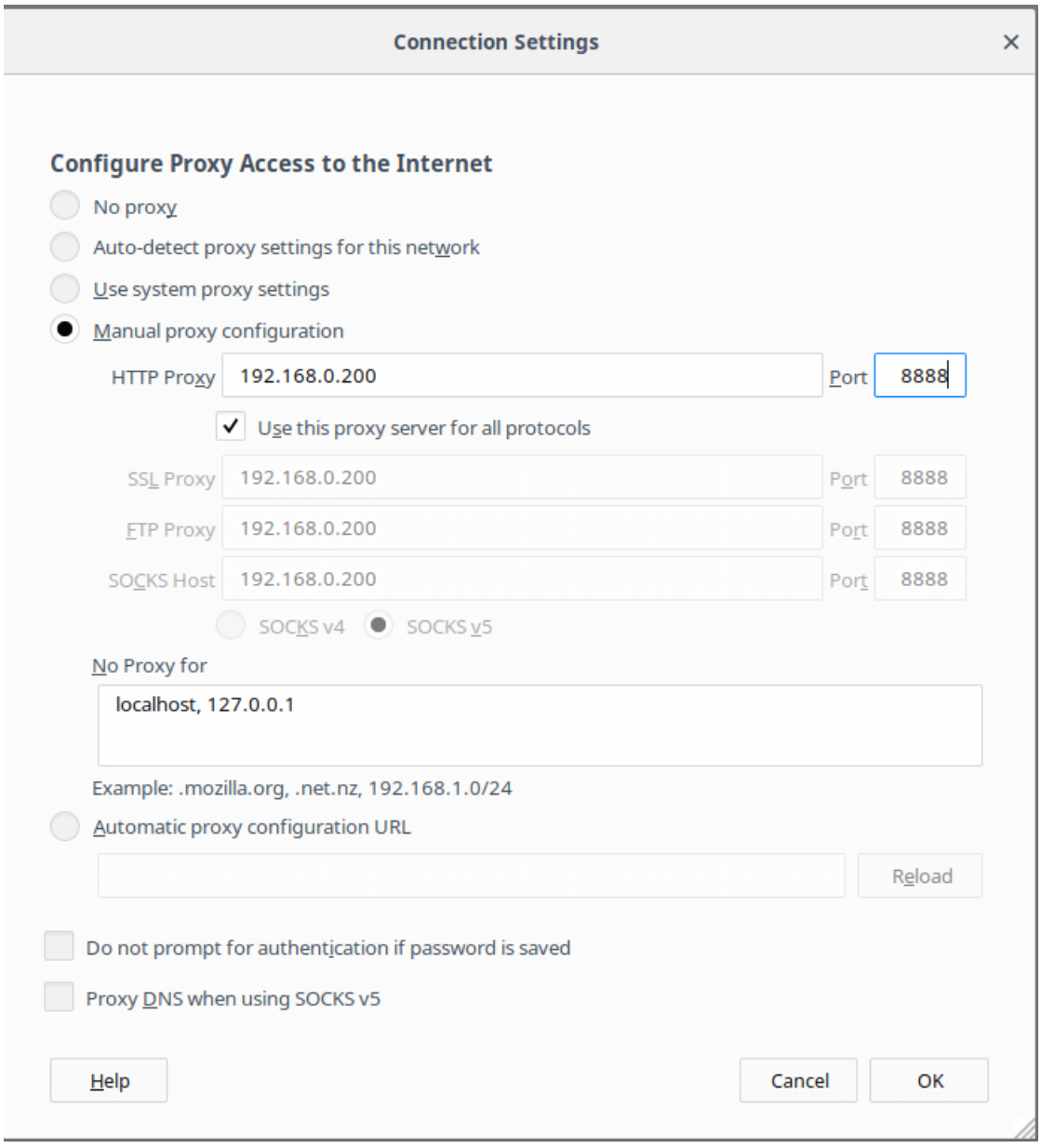
Change **http_access deny all** to **http_access allow all** to allow http traffic from browser access to proxy server.

Then restart squid:

```
$ sudo systemctl restart squid
```

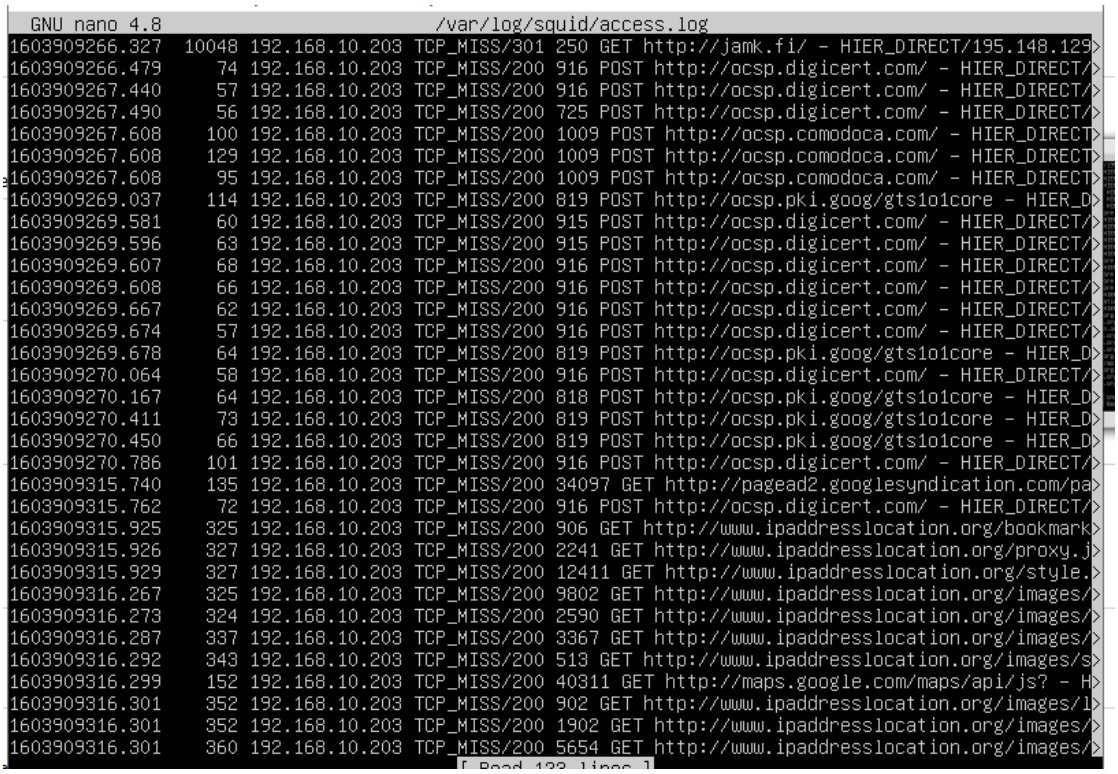
jamk.fi

In browser need to set manual proxy configuration and IP address and port which squid uses. Squid uses port 3128 by default.

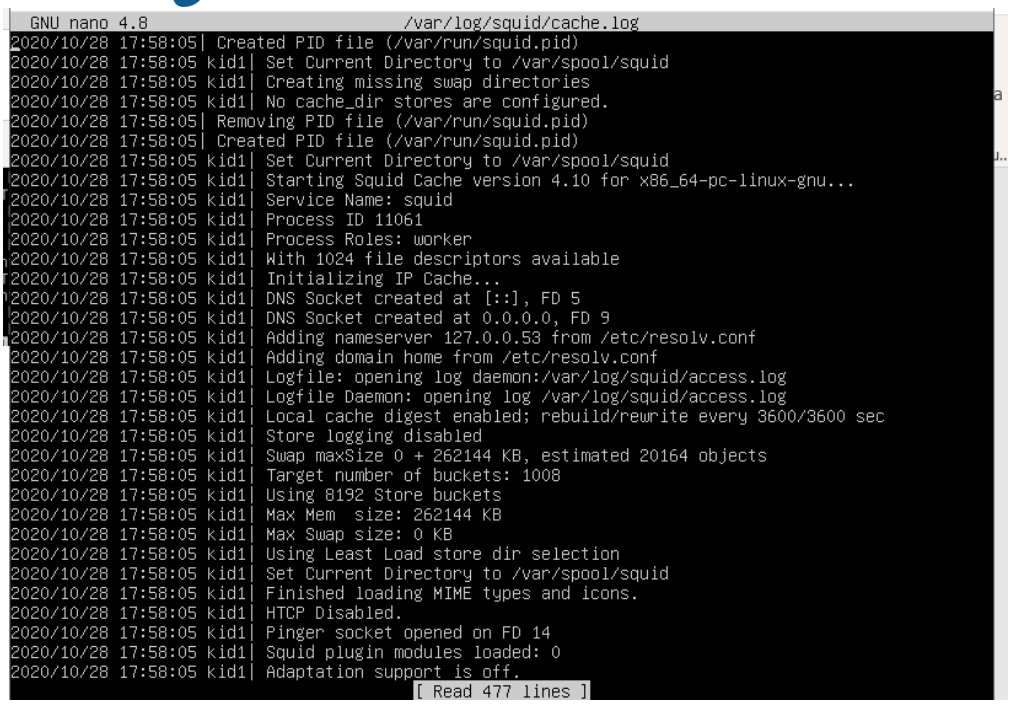


Then browse the internet and check the traffic from squid log file in:
/var/log/squid/access.log

jamk.fi



Squids caching file can be found in:
/var/log/squid/cache.log



27 TASK 2

Question:

Next learn how to block some certain sites using the proxy server. e.g. block www.jamk.fi Verify blocking to work correctly.

Answer:

In squid you can block web sites by creating file for addresses like:

```
$ sudo touch /etc/squid/blacklisted_sites.acl
```

Then add websites to file like:

```
.jamk.fi
```

First dot informs that squid blocks all references that sites include example www.jamk.fi

Then add configurations to:

```
$ sudo vim /etc/squid/squid.conf
```

After INSERT YOUR OWN RULES add:

```
acl bad_urls dstdomain "/etc/squid/blacklisted_sites.acl"
http_access deny bad_urls
```

Then restart squid.

28 TASK 3

Question:

Whats your opinion: Is there a benefit for having a cache system like this in your home network or in a network like JAMK has?

Answer:

In my home network there is just few people using the internet and I don’t have any services like webservers which could be accessed from the internet so I don’t see any benefits to use proxy in my home network.

In JAMK network there are much more users and it is good to protect the network from wrong kind of usage and forwarding proxy is also good for improving performance by caching.

jamk.fi

Exercise 10

Backups

Arttu Karhunen
n4924@student.jamk.fi

Exercise
Lokakuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Goal: Fix your machine to do backups
Needed stuff: Your Linux VM
Notes: Often people do not care of backups.

29 TASK 1

Question:

During this course we have set up quite a lot of stuff to the Linux server. Now it's time to make (almost) perfect backup solution locally to the Linux server. So: backup all important locations for the server. Use crontab to make this happen as often as required. Like: once a day incremental and once a week full backup. Read the lecture 10 slides regarding best practices.Use e.g. /backups/ folder.

Note that we are going to skip this time copying them to another secure location using rsync+ssh.
Explain how you did backups:

- what did you choose to backup
- did you use some scripts
- how did you utilize crontab
- Did you use tar ?

Answer:

1. First decided folder to backup. I already had folder /var/backups so that it is.
2. Then make python script to make backups from all files need at once.

```
  GNU nano 4.8                        /home/arttu/backup_python_daily.py
import os

os.system("sudo rsync -av --delete /home/arttu /var/backups/rsync/daily")
os.system("sudo rsync -av --delete /etc /var/backups/rsync/daily")
```

Daily backups from home folder and /etc folder

```
  GNU nano 4.8                          /home/arttu/backup_python.py
import os

os.system("sudo tar -cvpzf /var/backups/arttu.tar.gz -C /home/ arttu")
os.system("sudo tar -cvpzf /var/backups/etc.tar.gz -C / etc")
os.system("sudo tar -cvpzf /var/backups/var.tar.gz --exclude=var/backups --exclude=var/cache --excl
os.system("sudo tar -cvpzf /var/backups/arttu.tar.gz -C /usr/ local")
```

Weekly backups from:

- Home folder
- /etc folder because of config files
- /var folder because of those variable files of applications. Also excluded some files like cache and backups
- /usr/local because of the locally installed files

Used tar to zip the backups.

3. Test the backup by running the python file:

   # python3 /home/arttu/backup_python.py

   And

   # python3 /home/arttu/backup_python_daily.py

4. Check that backup files shows in /var/backups

```
arttu@ubuntu:/var/backups$ ls -la /var/backups
total 920
drwxr-xr-x  2 root root   4096 Nov  3 10:52 .
drwxr-xr-x 13 root root   4096 Jul 31 16:30 ..
-rw-r--r--  1 root root  71680 Oct 29 06:25 alternatives.tar.0
-rw-r--r--  1 root root  45226 Oct 28 17:57 apt.extended_states.0
-rw-r--r--  1 root root   4888 Oct 28 11:10 apt.extended_states.1.gz
-rw-r--r--  1 root root   4877 Oct 27 07:25 apt.extended_states.2.gz
-rw-r--r--  1 root root   4657 Oct 21 08:53 apt.extended_states.3.gz
-rw-r--r--  1 root root   3695 Oct 20 17:57 apt.extended_states.4.gz
-rw-r--r--  1 root root    568 Nov  3 11:04 arttu.tar.gz
-rw-r--r--  1 root root    268 Oct 20 17:41 dpkg.diversions.0
-rw-r--r--  1 root root    135 Oct 28 17:58 dpkg.statoverride.0
-rw-r--r--  1 root root 761578 Oct 28 17:58 dpkg.status.0
-rw-r--r--  1 root root     45 Nov  3 11:04 etc.tar.gz
-rw-r--r--  1 root root     45 Nov  3 11:04 var.tar.gz
arttu@ubuntu:/var/backups$ _
```

```
arttu@ubuntu:/var/backups/rsync/daily$ ls -la
total 16
drwxr-xr-x   4 root  root  4096 Nov  3 14:06 .
drwxr-xr-x   3 root  root  4096 Nov  3 14:05 ..
drwxrwx---   9 arttu arttu 4096 Nov  3 14:06 arttu
drwxr-xr-x 108 root  root  4096 Nov  3 13:16 etc
arttu@ubuntu:/var/backups/rsync/daily$
```

5. Configure cron:

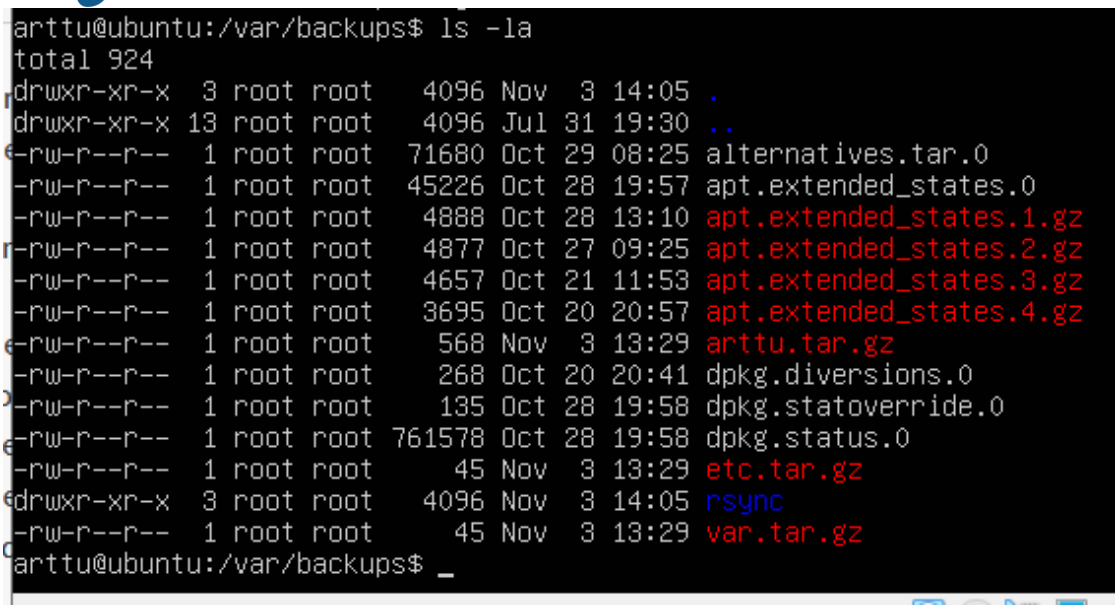
   # sudo crontab -e

   - Add line:

   29 13 * * * python3 /home/arttu/backup_python.py

6. Then checked that backup worked at 13.12 with:

   # ls -la /var/backups



7. Then add correct times for backups:

   - Rsync daily at 8:00 am

   00 8 * * * python3 /home/arttu/backup_python_daily.py

   - Full backup at 18:00 at every Sunday

   00 18 * * * python3 /home/arttu/backup_python.py

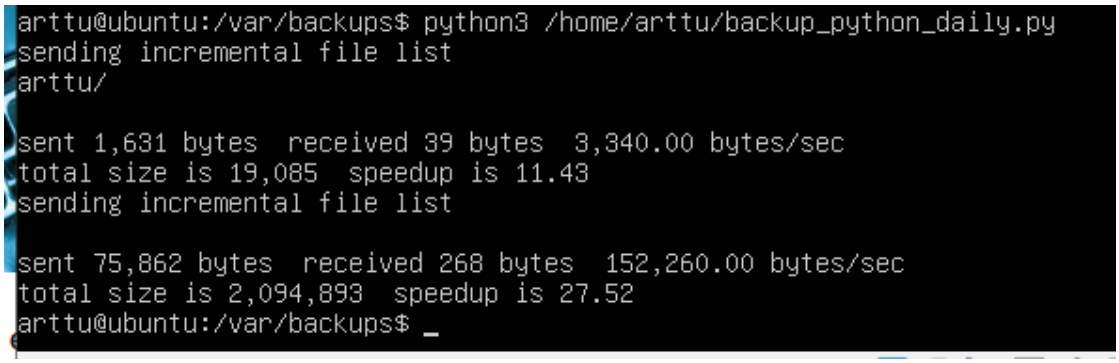
30 TASK 2

Question:

Verify that the backup you just made is nice and can be restored. No need to do th restoring process though, just that you verify that necessary information is backed up.

Answer:

Checking that daily python file work:



Test to restore tar files:

Restore home folder:

```
arttu@ubuntu:/var/backups$ sudo mkdir -p /var/backups/restore
arttu@ubuntu:/var/backups$ ls
alternatives.tar.0        apt.extended_states.2.gz  arttu.tar.gz         dpkg.status.0  rsync
apt.extended_states.0     apt.extended_states.3.gz  dpkg.diversions.0    etc.tar.gz     var.tar.gz
apt.extended_states.1.gz  apt.extended_states.4.gz  dpkg.statoverride.0  restore
arttu@ubuntu:/var/backups$ sudo tar -xvpzf /var/backups/arttu.tar.gz -C /var/backups/restore
local/
local/games/
local/man
local/etc/
local/include/
local/bin/
local/sbin/
local/src/
local/lib/
local/lib/python3.8/
local/lib/python3.8/dist-packages/
local/share/
local/share/xml/
local/share/xml/declaration/
local/share/xml/entities/
local/share/xml/misc/
local/share/xml/schema/
local/share/ca-certificates/
local/share/man/
local/share/fonts/
local/share/sgml/
local/share/sgml/declaration/
local/share/sgml/entities/
local/share/sgml/stylesheet/
local/share/sgml/misc/
local/share/sgml/dtd/
arttu@ubuntu:/var/backups$
```

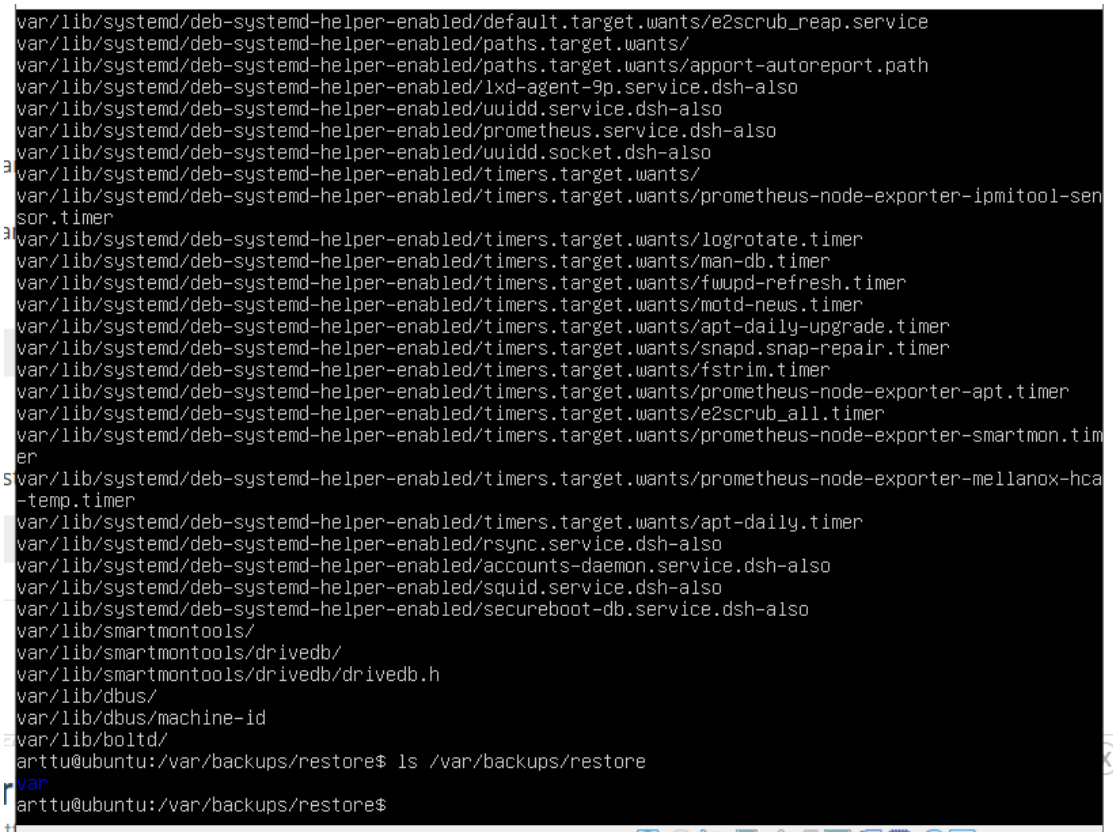
Restore etc:

jamk.fi

```
etc/console-setup/compose.GEORGIAN-ACADEMY.inc
etc/console-setup/compose.ISO-8859-11.inc
etc/console-setup/compose.IBM1133.inc
etc/console-setup/compose.ISO-8859-9.inc
etc/console-setup/compose.ISO-8859-7.inc
etc/console-setup/Uni2-Fixed16.psf.gz
etc/console-setup/compose.KOI8-R.inc
etc/console-setup/compose.ISO-8859-8.inc
etc/console-setup/compose.GEORGIAN-PS.inc
etc/console-setup/compose.TIS-620.inc
etc/console-setup/cached_setup_font.sh
etc/console-setup/compose.ISO-8859-3.inc
etc/console-setup/compose.ISO-8859-5.inc
etc/console-setup/cached_ISO-8859-1.acm.gz
etc/console-setup/compose.ARMSCII-8.inc
etc/console-setup/cached_setup_terminal.sh
etc/network/
etc/network/interfaces
etc/network/if-post-down.d/
etc/network/if-post-down.d/openvswitch
etc/network/if-up.d/
etc/network/if-up.d/ethtool
etc/network/if-pre-up.d/
etc/network/if-pre-up.d/openvswitch
etc/network/if-pre-up.d/ethtool
etc/rmt
etc/faucet/
etc/faucet/acls.yaml
etc/faucet/prometheus/
etc/faucet/prometheus/faucet.rules.yml
etc/faucet/prometheus/prometheus.yml
etc/faucet/gauge.yaml
etc/faucet/faucet.yaml
etc/faucet/ryu.conf
arttu@ubuntu:~$ ls /var/backups/restore
etc
arttu@ubuntu:~$
```

jamk.fi

Restore var:



Then remove restore directory:

sudo rm -r /var/backups/restore

jamk.fi

Exercise 11

Docker and Nextcloud

Arttu Karhunen
n4924@student.jamk.fi

Exercise
Marraskuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Goal: Install docker to your Linux
Needed stuff: Your Linux VM
Notes: This can be messy.

31 TASK 1

Question:

First we need to install the docker engine to the Linux. I used https://linuxconfig.org/how-to-install-docker-in-rhel-8
Summary of that:
install repository for docker dnf config-manager --add-repo=https://download.docker.com/linux/centos/docker-ce.repo
install the docker engine: dnf install docker-ce-3:18.09.1-3.el7
Start the engine! systemctl start docker
Test whether it works or not: docker run hello-world

Answer:

First install repository for docker:

```
# sudo dnf config-manager --add-repo=https://down-
load.docker.com/linux/centos/docker-ce.repo
```

Then install docker engine:

```
Sudo dnf install docker-ce
```

Then start docker:

```
# sudo systemctl start docker
```

Then run Hello World:

```
# sudo docker run hello-world
```

32 TASK 2

Question:

Search what images do you have in your docker installation. Also what containers do you have running.

Answer:

Images:

Containers:

33 TASK 3

Question:

Launch a Nextcloud docker image and insert a port forwarding for it. While the next-cloud is running, check again the list of containers. Then start how you can go inside the container and modify it on-the-fly.

Answer:

Start nextcloud container and make portforward rule from host port 8080 to contain-ers port 80:

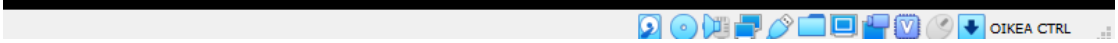
 # docker run -d -p 8080:80 nextcloud

Check images and containers:

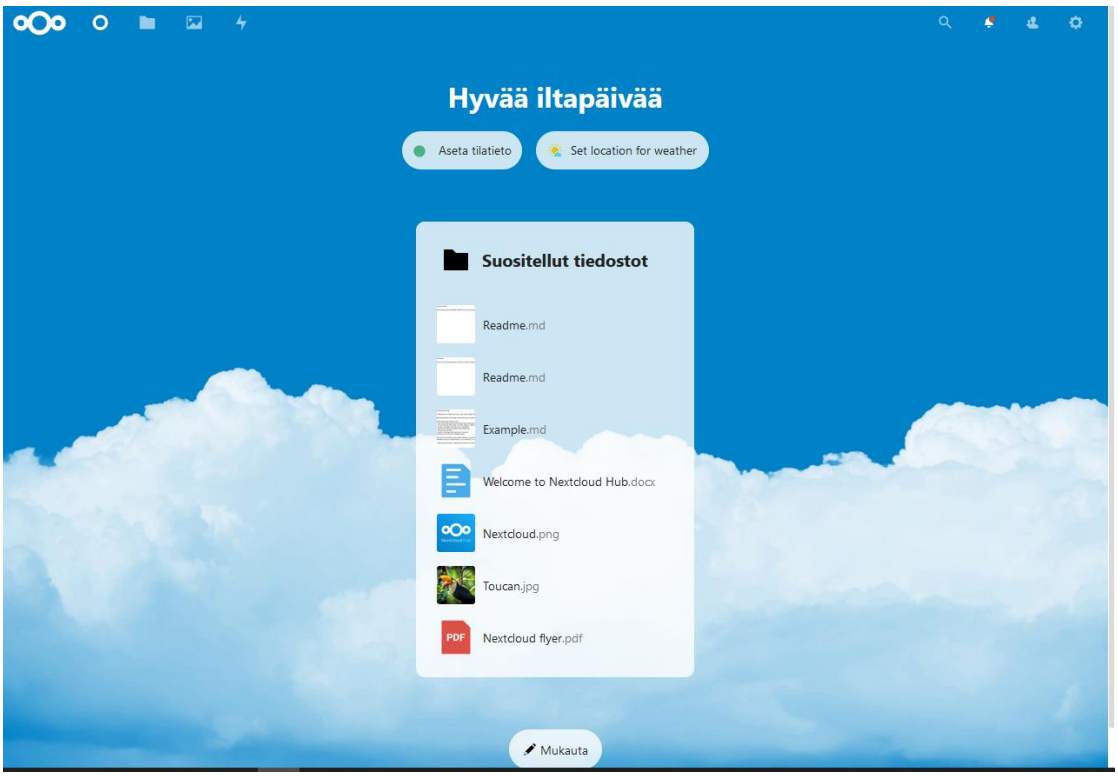
```
[arttu@centos ~]$ sudo docker images
[sudo] password for arttu:
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
nextcloud           latest              0fe69d55da2d        4 days ago          811MB
hello-world         latest              bf756fb1ae65        10 months ago       13.3kB
[arttu@centos ~]$ sudo docker ps -a
CONTAINER ID        IMAGE               COMMAND                  CREATED             STATUS
            PORTS                    NAMES
9abf355ec2ca        nextcloud           "/entrypoint.sh apac…"   3 minutes ago       Up 3 minutes
            0.0.0.0:8080->80/tcp     hungry_booth
d5242c3efacc        hello-world         "/hello"                 42 minutes ago      Exited (0) 42 m
inutes ago                           wonderful_mendeleev
[arttu@centos ~]$
```

Testing connection to nextcloud:

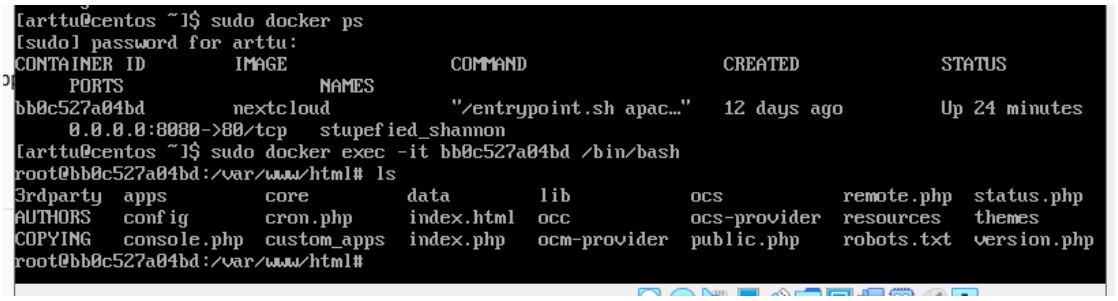
```
[arttu@centos ~]$ wget http://localhost:8080
--2020-11-04 11:59:06--  http://localhost:8080/
Resolving localhost (localhost)... ::1, 127.0.0.1
Connecting to localhost (localhost)|::1|:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6832 (6.7K) [text/html]
Saving to: 'index.html'

index.html              100%[===================================>]   6.67K  --.-KB/s    in 0s

2020-11-04 11:59:07 (491 MB/s) - 'index.html' saved [6832/6832]

[arttu@centos ~]$ _
```



Testing connection with browser: http://ip_address _of_the_host:8080



Test how to get inside docker container to look at the bash shell:



TÄMÄ ON VIELÄ KESKEN

34 TASK 4

Question:

It is highly possible that the Nextcloud is running in plain HTTP. Enable the HTTPS as you see the best. You can either build it directly to the docker container or use some other method like reverse proxy.

Answer:

I used Nginx reverse proxy to forward https traffic to nextcloud.
First installed nginx to docker container using ports 443 both host and container:

 # Docker run -d –name proxy -p 443:443 nginx

I used self created certificate. Created ceritficates to nginx container:

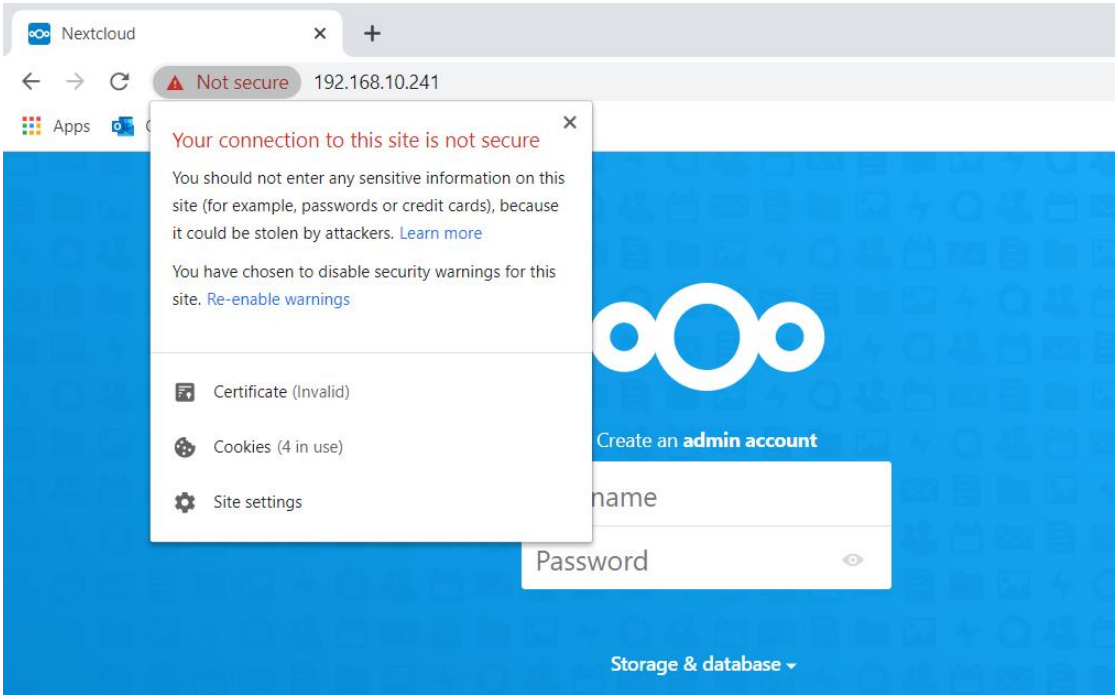
 # openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ngnix/ssl/example.key -out /etc/ngnix/ssl/example.crt

Then change conf in container file:

/etc/nginx/conf.d/default.conf

```
server {
    listen       443 ssl;
    listen  [::]:443;
    server_name  localhost;

    ssl_certificate /etc/nginx/ssl/example.crt;
    ssl_certificate_key /etc/nginx/ssl/example.key;
    #charset koi8-r;
    #access_log  /var/log/nginx/host.access.log  main;

    location / {
        proxy_pass http://172.17.0.3;
    }
```

Added certificate and forward to nextcloud container



35 TASK 5

Question:

Goal of this is to grab a docker image, launch a container from that, edit something and save the changes to another image. Next grab new docker image to your machine:
Alpine Linux https://hub.docker.com/_/alpine
Install something there using apk Next use e.g. commit to save the current container to image. Verify that you have a new container that holds modifications you made. This is useful for instance in cases where you are building some CI/CD image and its getting launched several times and needs some specific software. There is no point in re-installing the software every time the container starts.

Answer:

First pull and run docker image:

```
# docker run -d --name alpine -it alpine:3
```

Execute shell with:

```
# docker container exec -it alpine /bin/sh
```

Then install python with apk:

```
# apk add python3
```

Then exit container:

```
# exit
```

Then make another image with commit:

```
# docker commit alpine new_alpine
Create container from image:
# docker run -d --name alpine_new -it new_alpinedoc
```

Open new_alpine shell and check python with:

```
# docker container exec -it new_alpine /bin/sh
# python3 -version
```