jamk.fi

Labra 5

Troubleshooting

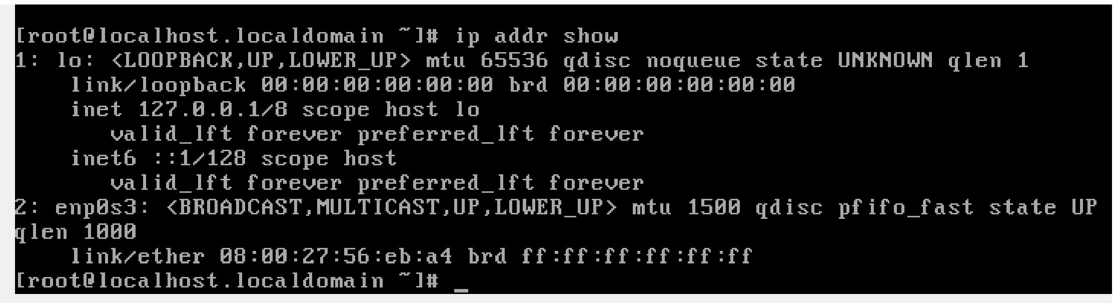
Alexander Andreev
K8684
TTV16S3

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Sisältö

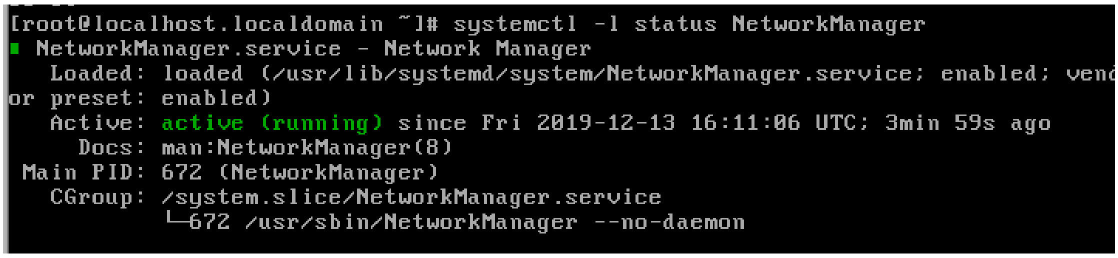
1 Troubleshooting

As we can see, IP address is missing.

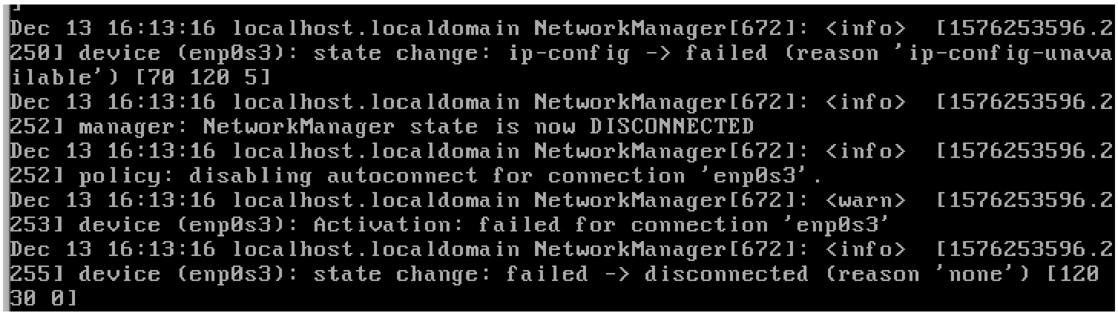


```
[root@localhost.localdomain ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
qlen 1000
    link/ether 08:00:27:56:eb:a4 brd ff:ff:ff:ff:ff:ff
[root@localhost.localdomain ~]# _
```

Checking Network manager status

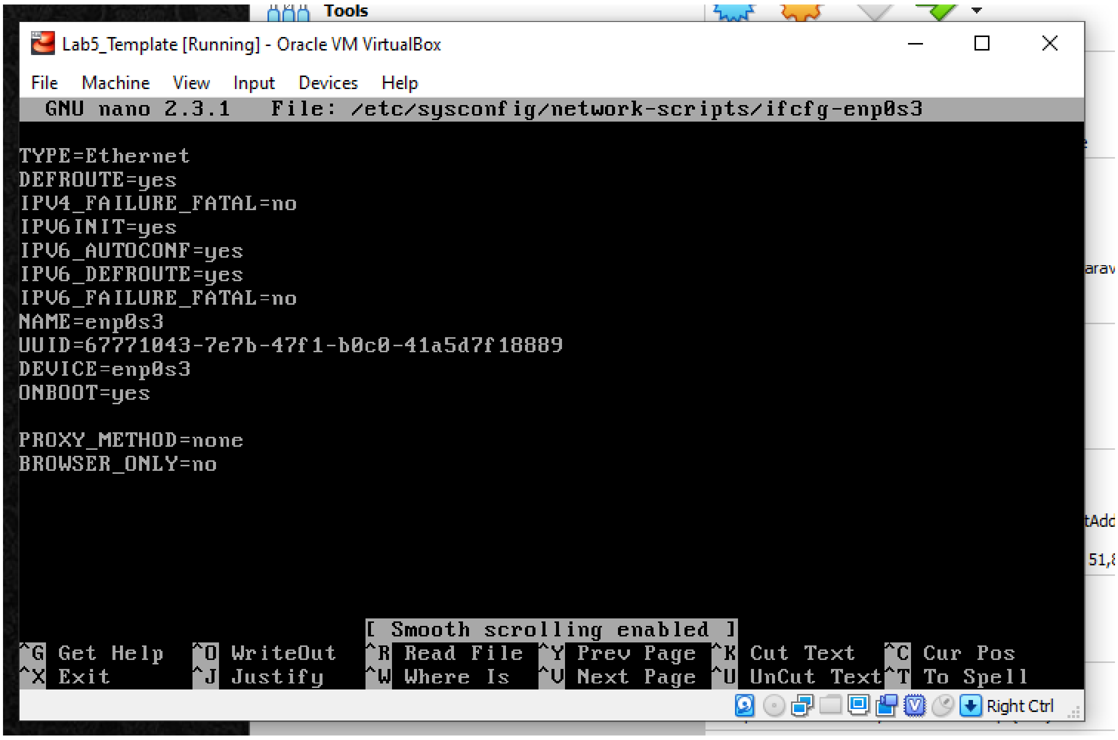


```
[root@localhost.localdomain ~]# systemctl -l status NetworkManager
● NetworkManager.service - Network Manager
   Loaded: loaded (/usr/lib/systemd/system/NetworkManager.service; enabled; vend
or preset: enabled)
   Active: active (running) since Fri 2019-12-13 16:11:06 UTC; 3min 59s ago
     Docs: man:NetworkManager(8)
 Main PID: 672 (NetworkManager)
   CGroup: /system.slice/NetworkManager.service
           └─672 /usr/sbin/NetworkManager --no-daemon
```



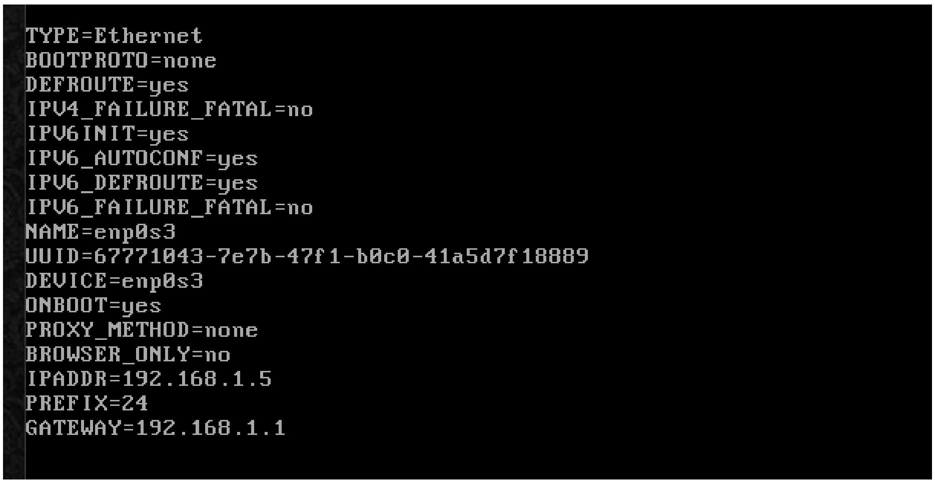
```
Dec 13 16:13:16 localhost.localdomain NetworkManager[672]: <info>  [1576253596.2
250] device (enp0s3): state change: ip-config -> failed (reason 'ip-config-unava
ilable') [70 120 5]
Dec 13 16:13:16 localhost.localdomain NetworkManager[672]: <info>  [1576253596.2
252] manager: NetworkManager state is now DISCONNECTED
Dec 13 16:13:16 localhost.localdomain NetworkManager[672]: <info>  [1576253596.2
252] policy: disabling autoconnect for connection 'enp0s3'.
Dec 13 16:13:16 localhost.localdomain NetworkManager[672]: <warn>  [1576253596.2
253] device (enp0s3): Activation: failed for connection 'enp0s3'
Dec 13 16:13:16 localhost.localdomain NetworkManager[672]: <info>  [1576253596.2
255] device (enp0s3): state change: failed -> disconnected (reason 'none') [120
30 0]
```

It doesn't give IP because it is not defined in conf file



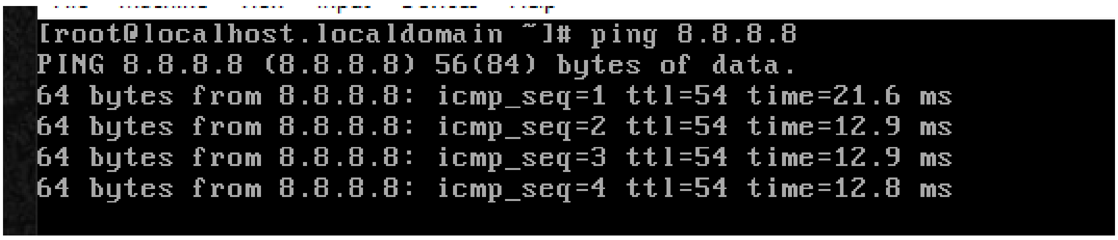
```
  GNU nano 2.3.1    File: /etc/sysconfig/network-scripts/ifcfg-enp0s3

TYPE=Ethernet
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
NAME=enp0s3
UUID=67771043-7e7b-47f1-b0c0-41a5d7f18889
DEVICE=enp0s3
ONBOOT=yes

PROXY_METHOD=none
BROWSER_ONLY=no




                            [ Smooth scrolling enabled ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

New conf

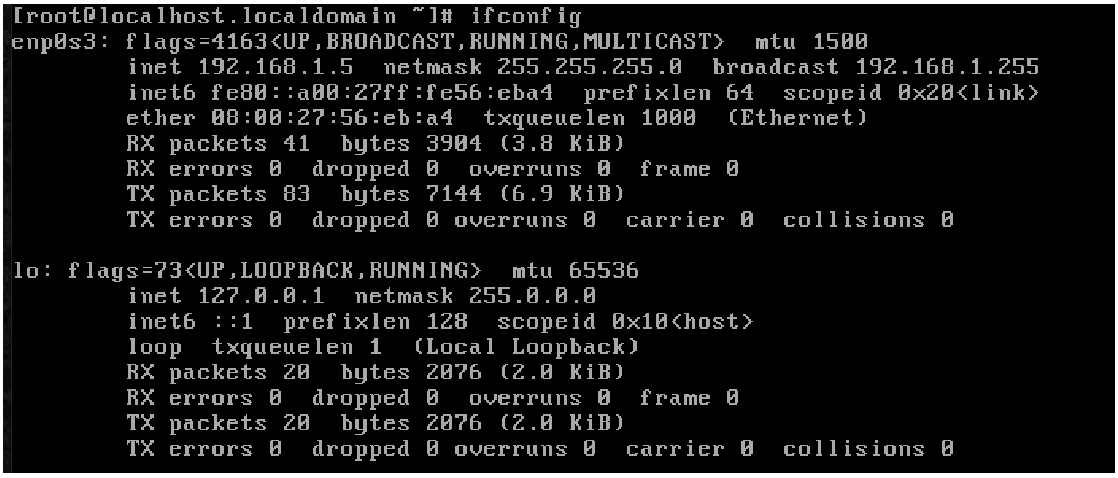


```
TYPE=Ethernet
BOOTPROTO=none
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
NAME=enp0s3
UUID=67771043-7e7b-47f1-b0c0-41a5d7f18889
DEVICE=enp0s3
ONBOOT=yes
PROXY_METHOD=none
BROWSER_ONLY=no
IPADDR=192.168.1.5
PREFIX=24
GATEWAY=192.168.1.1
```

Network works again after systemctl restart NetworkManager.service



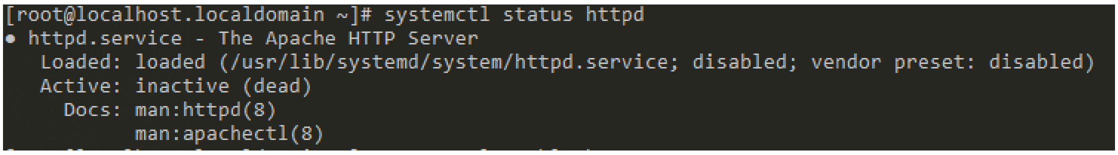
```
[root@localhost.localdomain ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=54 time=21.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=54 time=12.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=54 time=12.9 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=54 time=12.8 ms
```



```
[root@localhost.localdomain ~]# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.5  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe56:eba4  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:56:eb:a4  txqueuelen 1000  (Ethernet)
        RX packets 41  bytes 3904 (3.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 83  bytes 7144 (6.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 20  bytes 2076 (2.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 2076 (2.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

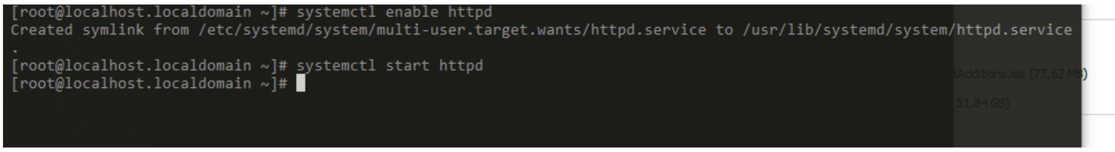
2 Service availability

Httpd service is currently inactive



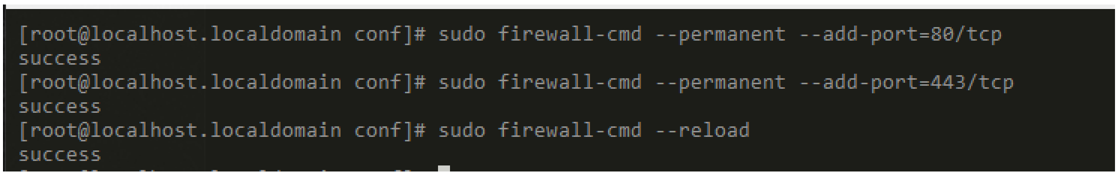
```
[root@localhost.localdomain ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:httpd(8)
           man:apachectl(8)
```

Enabling it, and restarting



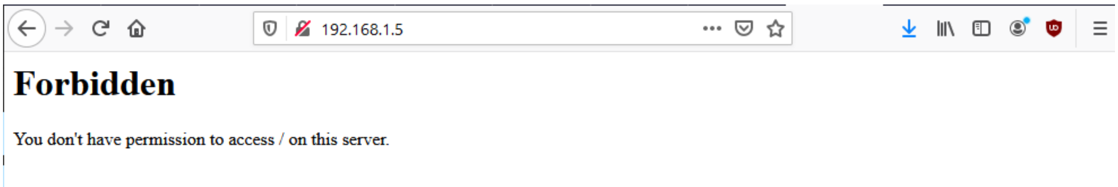
```
[root@localhost.localdomain ~]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service
.
[root@localhost.localdomain ~]# systemctl start httpd
[root@localhost.localdomain ~]# █
```

Next step is to allow default ports 80 and 443 in firewall



```
[root@localhost.localdomain conf]# sudo firewall-cmd --permanent --add-port=80/tcp
success
[root@localhost.localdomain conf]# sudo firewall-cmd --permanent --add-port=443/tcp
success
[root@localhost.localdomain conf]# sudo firewall-cmd --reload
success
```

After allowing default ports

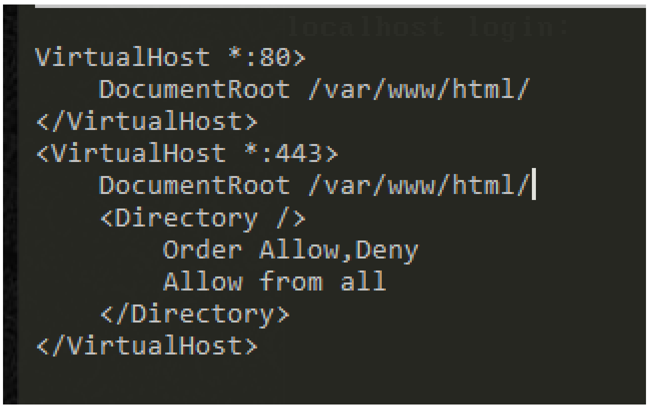


Forbidden

You don't have permission to access / on this server.

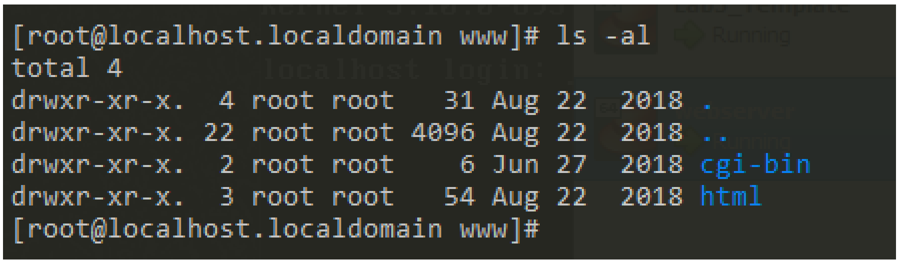
3 Access denied

Have to configure httpd.conf file. Because no extra instructions are given, I assume path can be accessed from anywhere, so no need to configure .htaccess authentication. Using custom conf file allow access from anywhere



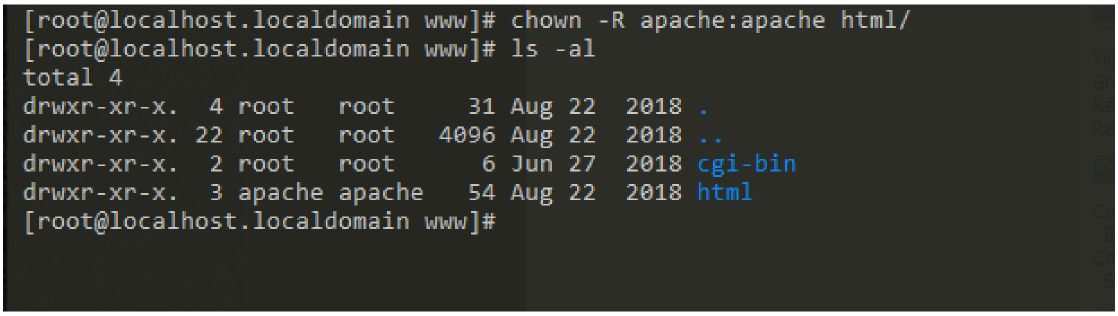
```
VirtualHost *:80>
    DocumentRoot /var/www/html/
</VirtualHost>
<VirtualHost *:443>
    DocumentRoot /var/www/html/
    <Directory />
        Order Allow,Deny
        Allow from all
    </Directory>
</VirtualHost>
```

Was searching in the wrong place… here is the problem, Apache doesn't have permission to access required folder



```
[root@localhost.localdomain www]# ls -al
total 4
drwxr-xr-x.  4 root root   31 Aug 22  2018 .
drwxr-xr-x. 22 root root 4096 Aug 22  2018 ..
drwxr-xr-x.  2 root root    6 Jun 27  2018 cgi-bin
drwxr-xr-x.  3 root root   54 Aug 22  2018 html
[root@localhost.localdomain www]#
```

Changing ownership

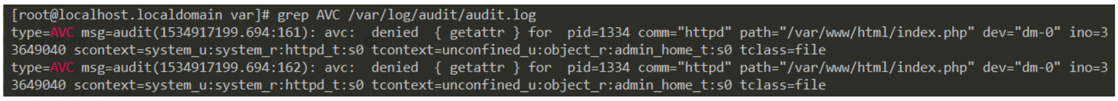


```
[root@localhost.localdomain www]# chown -R apache:apache html/
[root@localhost.localdomain www]# ls -al
total 4
drwxr-xr-x.  4 root   root     31 Aug 22  2018 .
drwxr-xr-x. 22 root   root   4096 Aug 22  2018 ..
drwxr-xr-x.  2 root   root      6 Jun 27  2018 cgi-bin
drwxr-xr-x.  3 apache apache   54 Aug 22  2018 html
[root@localhost.localdomain www]#
```

Hmm.. still nothing.. Took a lot of time to understand what problem is possible in SELinux context

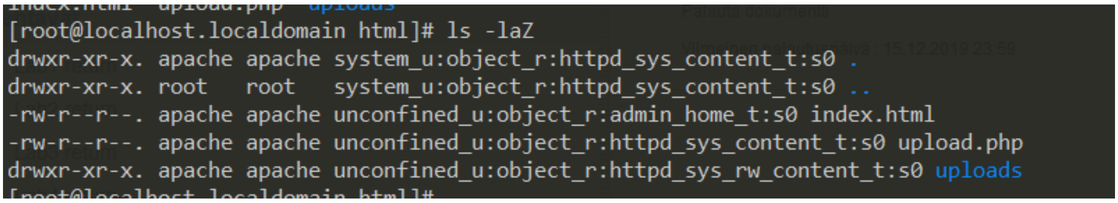
Checking with `grep AVC /var/log/audit/audit.log`

Jep finally, seems like this is an error, a lot of httpd errors



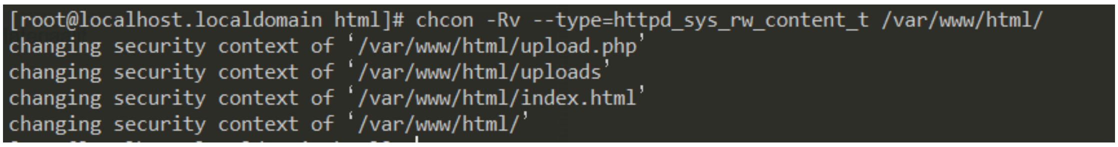
```
[root@localhost.localdomain var]# grep AVC /var/log/audit/audit.log
type=AVC msg=audit(1534917199.694:161): avc:  denied  { getattr } for  pid=1334 comm="httpd" path="/var/www/html/index.php" dev="dm-0" ino=3
3649040 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:admin_home_t:s0 tclass=file
type=AVC msg=audit(1534917199.694:162): avc:  denied  { getattr } for  pid=1334 comm="httpd" path="/var/www/html/index.php" dev="dm-0" ino=3
3649040 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:admin_home_t:s0 tclass=file
```

Here we can see the reason why nothing works



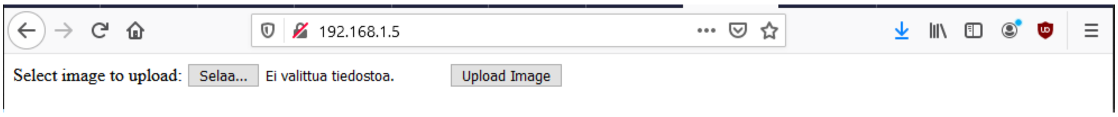
```
index.html  upload.php  uploads
[root@localhost.localdomain html]# ls -laZ
drwxr-xr-x. apache apache system_u:object_r:httpd_sys_content_t:s0 .
drwxr-xr-x. root   root   system_u:object_r:httpd_sys_content_t:s0 ..
-rw-r--r--. apache apache unconfined_u:object_r:admin_home_t:s0 index.html
-rw-r--r--. apache apache unconfined_u:object_r:httpd_sys_content_t:s0 upload.php
drwxr-xr-x. apache apache unconfined_u:object_r:httpd_sys_rw_content_t:s0 uploads
[root@localhost.localdomain html]#
```

Changing context of files



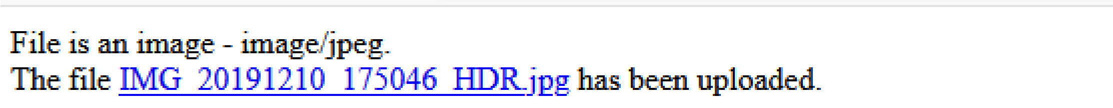
```
[root@localhost.localdomain html]# chcon -Rv --type=httpd_sys_rw_content_t /var/www/html/
changing security context of '/var/www/html/upload.php'
changing security context of '/var/www/html/uploads'
changing security context of '/var/www/html/index.html'
changing security context of '/var/www/html/'
```

Now it finally starts to work

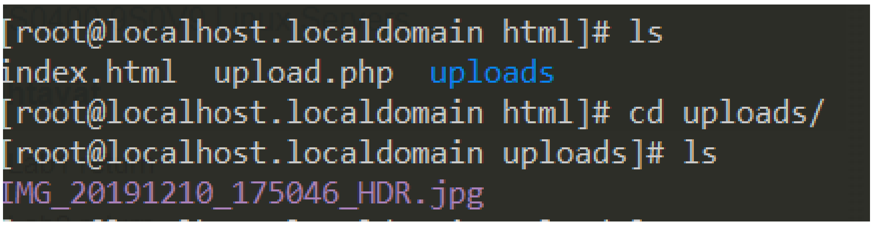


Select image to upload: Selaa... Ei valittua tiedostoa. Upload Image

Here we have step where upload should fail, but because I already changed ownership to apache while trying to fix previous problem, seems like now everything works as it should.



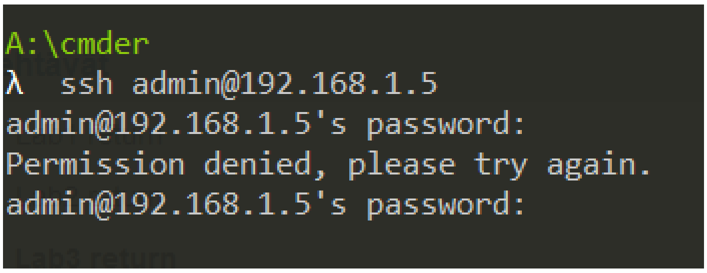
File is an image - image/jpeg.
The file IMG_20191210_175046_HDR.jpg has been uploaded.



```
[root@localhost.localdomain html]# ls
index.html  upload.php  uploads
[root@localhost.localdomain html]# cd uploads/
[root@localhost.localdomain uploads]# ls
IMG_20191210_175046_HDR.jpg
```

4 Login

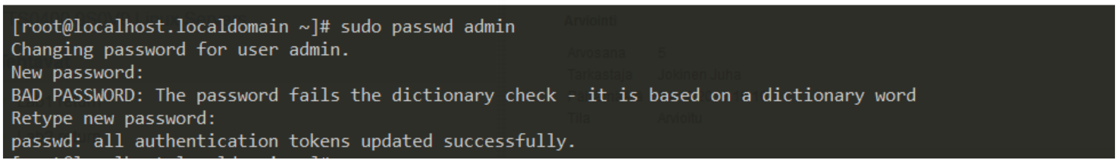
Credentials don't work when trying to connect…



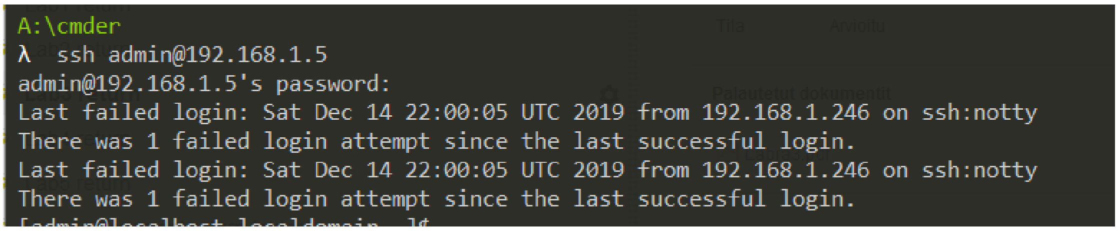
```
A:\cmder
λ  ssh admin@192.168.1.5
admin@192.168.1.5's password:
Permission denied, please try again.
admin@192.168.1.5's password:
```

Most simple solution. Because we can't login as user, and password information is hashed so we cant check it, we can just change password as root to desired one. Maybe there was just a typo/misspelling during password creation.

(sudo not necessary, just used to it, even logged in root)

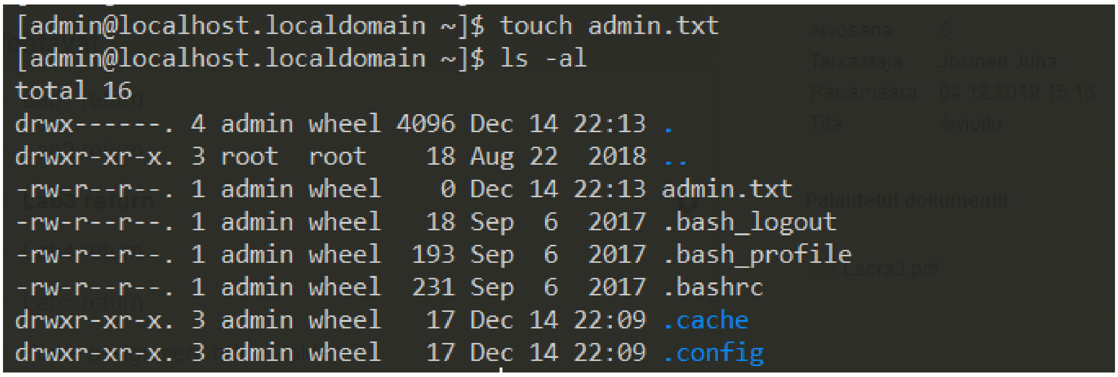


```
[root@localhost.localdomain ~]# sudo passwd admin
Changing password for user admin.
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
passwd: all authentication tokens updated successfully.
```

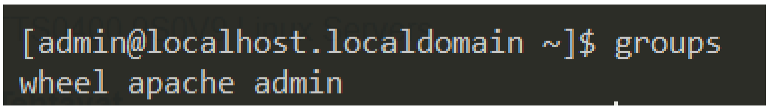


```
A:\cmder
λ  ssh admin@192.168.1.5
admin@192.168.1.5's password:
Last failed login: Sat Dec 14 22:00:05 UTC 2019 from 192.168.1.246 on ssh:notty
There was 1 failed login attempt since the last successful login.
Last failed login: Sat Dec 14 22:00:05 UTC 2019 from 192.168.1.246 on ssh:notty
There was 1 failed login attempt since the last successful login.
[admin@localhost.localdomain ~]$
```

Creating new file



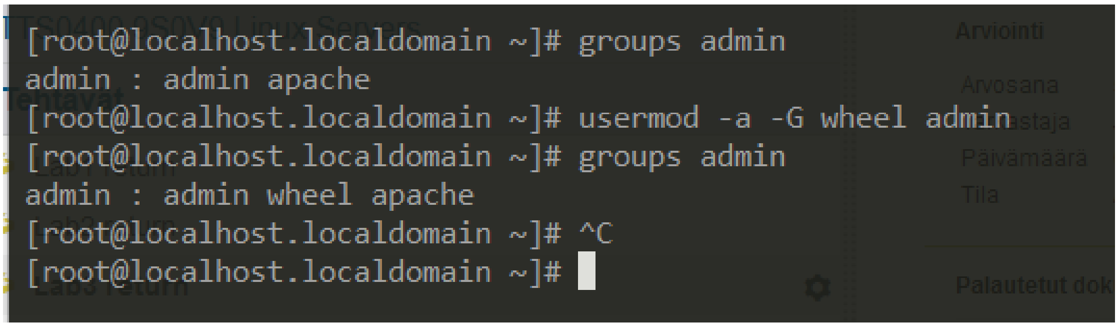
```
[admin@localhost.localdomain ~]$ touch admin.txt
[admin@localhost.localdomain ~]$ ls -al
total 16
drwx------. 4 admin wheel 4096 Dec 14 22:13 .
drwxr-xr-x. 3 root  root    18 Aug 22  2018 ..
-rw-r--r--. 1 admin wheel    0 Dec 14 22:13 admin.txt
-rw-r--r--. 1 admin wheel   18 Sep  6  2017 .bash_logout
-rw-r--r--. 1 admin wheel  193 Sep  6  2017 .bash_profile
-rw-r--r--. 1 admin wheel  231 Sep  6  2017 .bashrc
drwxr-xr-x. 3 admin wheel   17 Dec 14 22:09 .cache
drwxr-xr-x. 3 admin wheel   17 Dec 14 22:09 .config
```



```
[admin@localhost.localdomain ~]$ groups
wheel apache admin
```

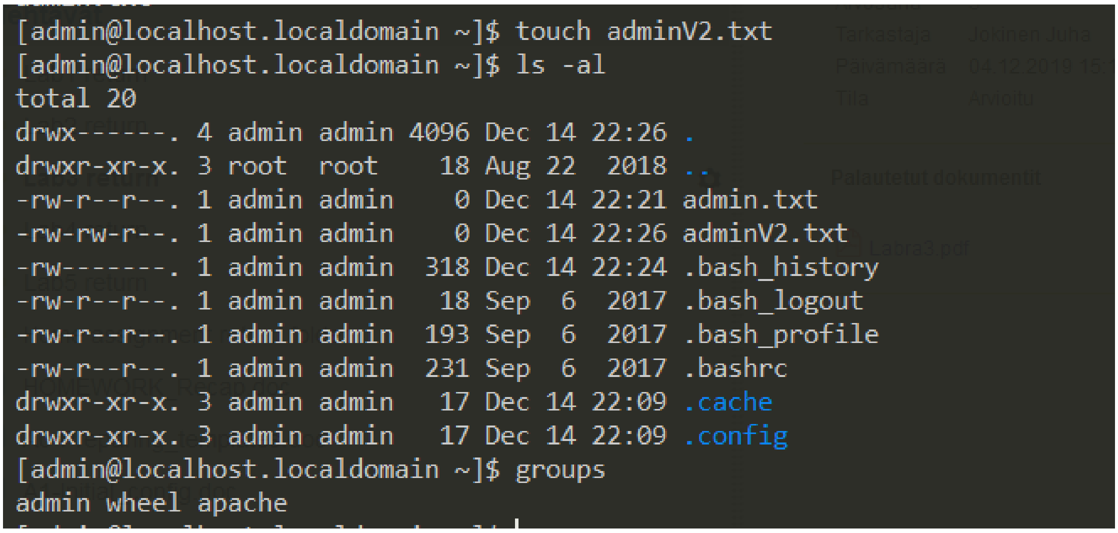
Seems like user has wrong primary groups

Changing primary group with usermod -g. Adding wheel as secondary group



```
[root@localhost.localdomain ~]# groups admin
admin : admin apache
[root@localhost.localdomain ~]# usermod -a -G wheel admin
[root@localhost.localdomain ~]# groups admin
admin : admin wheel apache
[root@localhost.localdomain ~]# ^C
[root@localhost.localdomain ~]#
```

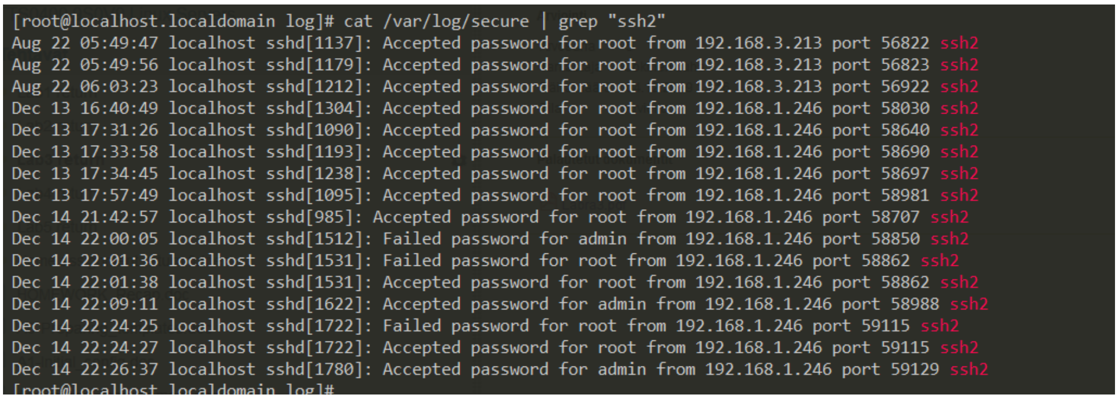
User still belongs to groups apache and wheel, but now group for created files is admin



```
[admin@localhost.localdomain ~]$ touch adminV2.txt
[admin@localhost.localdomain ~]$ ls -al
total 20
drwx------. 4 admin admin 4096 Dec 14 22:26 .
drwxr-xr-x. 3 root  root    18 Aug 22  2018 ..
-rw-r--r--. 1 admin admin    0 Dec 14 22:21 admin.txt
-rw-rw-r--. 1 admin admin    0 Dec 14 22:26 adminV2.txt
-rw-------. 1 admin admin  318 Dec 14 22:24 .bash_history
-rw-r--r--. 1 admin admin   18 Sep  6  2017 .bash_logout
-rw-r--r--. 1 admin admin  193 Sep  6  2017 .bash_profile
-rw-r--r--. 1 admin admin  231 Sep  6  2017 .bashrc
drwxr-xr-x. 3 admin admin   17 Dec 14 22:09 .cache
drwxr-xr-x. 3 admin admin   17 Dec 14 22:09 .config
[admin@localhost.localdomain ~]$ groups
admin wheel apache
```

5 SSH access

Looks like last loggin from ssh was made on August 22



```
[root@localhost.localdomain log]# cat /var/log/secure | grep "ssh2"
Aug 22 05:49:47 localhost sshd[1137]: Accepted password for root from 192.168.3.213 port 56822 ssh2
Aug 22 05:49:56 localhost sshd[1179]: Accepted password for root from 192.168.3.213 port 56823 ssh2
Aug 22 06:03:23 localhost sshd[1212]: Accepted password for root from 192.168.3.213 port 56922 ssh2
Dec 13 16:40:49 localhost sshd[1304]: Accepted password for root from 192.168.1.246 port 58030 ssh2
Dec 13 17:31:26 localhost sshd[1090]: Accepted password for root from 192.168.1.246 port 58640 ssh2
Dec 13 17:33:58 localhost sshd[1193]: Accepted password for root from 192.168.1.246 port 58690 ssh2
Dec 13 17:34:45 localhost sshd[1238]: Accepted password for root from 192.168.1.246 port 58697 ssh2
Dec 13 17:57:49 localhost sshd[1095]: Accepted password for root from 192.168.1.246 port 58981 ssh2
Dec 14 21:42:57 localhost sshd[985]: Accepted password for root from 192.168.1.246 port 58707 ssh2
Dec 14 22:00:05 localhost sshd[1512]: Failed password for admin from 192.168.1.246 port 58850 ssh2
Dec 14 22:01:36 localhost sshd[1531]: Failed password for root from 192.168.1.246 port 58862 ssh2
Dec 14 22:01:38 localhost sshd[1531]: Accepted password for root from 192.168.1.246 port 58862 ssh2
Dec 14 22:09:11 localhost sshd[1622]: Accepted password for admin from 192.168.1.246 port 58988 ssh2
Dec 14 22:24:25 localhost sshd[1722]: Failed password for root from 192.168.1.246 port 59115 ssh2
Dec 14 22:24:27 localhost sshd[1722]: Accepted password for root from 192.168.1.246 port 59115 ssh2
Dec 14 22:26:37 localhost sshd[1780]: Accepted password for admin from 192.168.1.246 port 59129 ssh2
[root@localhost.localdomain log]#
```