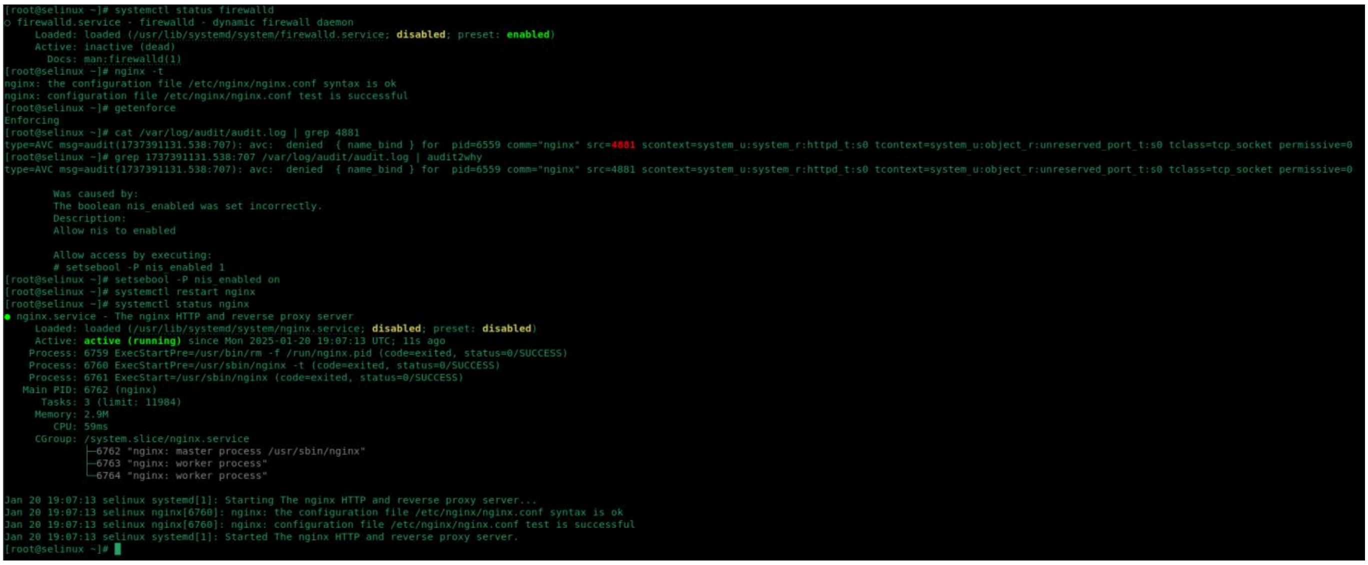
ДЗ «Практика с SELinux»

- Часть 1. Запуск nginx на нестандартном порту

1. Проверка конфигурации firewall и nginx;

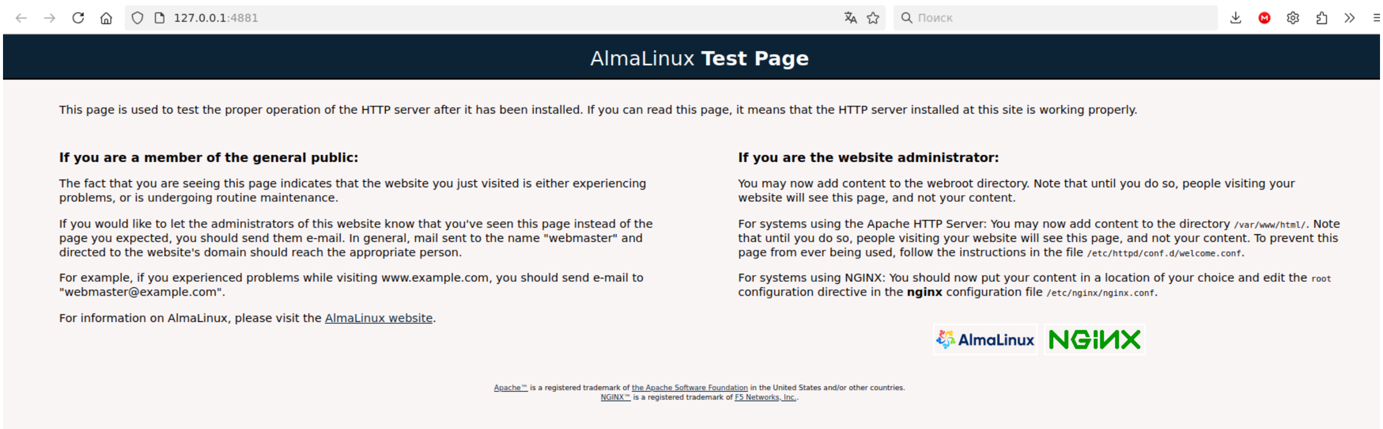
   Разрешение SELinux работы nginx на порту TCP 4881 с помощью переключателей setsebool:

   setsebool -P nis_enabled on



```
[root@selinux ~]# systemctl status firewalld
○ firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; preset: enabled)
     Active: inactive (dead)
       Docs: man:firewalld(1)
[root@selinux ~]# nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
[root@selinux ~]# getenforce
Enforcing
[root@selinux ~]# cat /var/log/audit/audit.log | grep 4881
type=AVC msg=audit(1737391131.538:707): avc:  denied  { name_bind } for  pid=6559 comm="nginx" src=4881 scontext=system_u:system_r:httpd_t:s0 tcontext=system_u:object_r:unreserved_port_t:s0 tclass=tcp_socket permissive=0
[root@selinux ~]# grep 1737391131.538:707 /var/log/audit/audit.log | audit2why
type=AVC msg=audit(1737391131.538:707): avc:  denied  { name_bind } for  pid=6559 comm="nginx" src=4881 scontext=system_u:system_r:httpd_t:s0 tcontext=system_u:object_r:unreserved_port_t:s0 tclass=tcp_socket permissive=0

        Was caused by:
        The boolean nis_enabled was set incorrectly.
        Description:
        Allow nis to enabled

        Allow access by executing:
        # setsebool -P nis_enabled 1
[root@selinux ~]# setsebool -P nis_enabled on
[root@selinux ~]# systemctl restart nginx
[root@selinux ~]# systemctl status nginx
● nginx.service - The nginx HTTP and reverse proxy server
     Loaded: loaded (/usr/lib/systemd/system/nginx.service; disabled; preset: disabled)
     Active: active (running) since Mon 2025-01-20 19:07:13 UTC; 11s ago
    Process: 6759 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=0/SUCCESS)
    Process: 6760 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=0/SUCCESS)
    Process: 6761 ExecStart=/usr/sbin/nginx (code=exited, status=0/SUCCESS)
   Main PID: 6762 (nginx)
      Tasks: 3 (limit: 11984)
     Memory: 2.9M
        CPU: 59ms
     CGroup: /system.slice/nginx.service
             ├─6762 "nginx: master process /usr/sbin/nginx"
             ├─6763 "nginx: worker process"
             └─6764 "nginx: worker process"

Jan 20 19:07:13 selinux systemd[1]: Starting The nginx HTTP and reverse proxy server...
Jan 20 19:07:13 selinux nginx[6760]: nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
Jan 20 19:07:13 selinux nginx[6760]: nginx: configuration file /etc/nginx/nginx.conf test is successful
Jan 20 19:07:13 selinux systemd[1]: Started The nginx HTTP and reverse proxy server.
[root@selinux ~]# 
```

2. Проверка работы nginx после setsebool:



AlmaLinux **Test Page**

This page is used to test the proper operation of the HTTP server after it has been installed. If you can read this page, it means that the HTTP server installed at this site is working properly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

For information on AlmaLinux, please visit the AlmaLinux website.

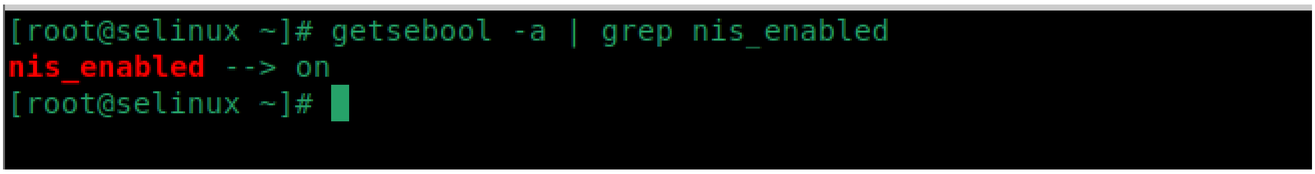
If you are the website administrator:

You may now add content to the webroot directory. Note that until you do so, people visiting your website will see this page, and not your content.

For systems using the Apache HTTP Server: You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

For systems using NGINX: You should now put your content in a location of your choice and edit the `root` configuration directive in the **nginx** configuration file `/etc/nginx/nginx.conf`.

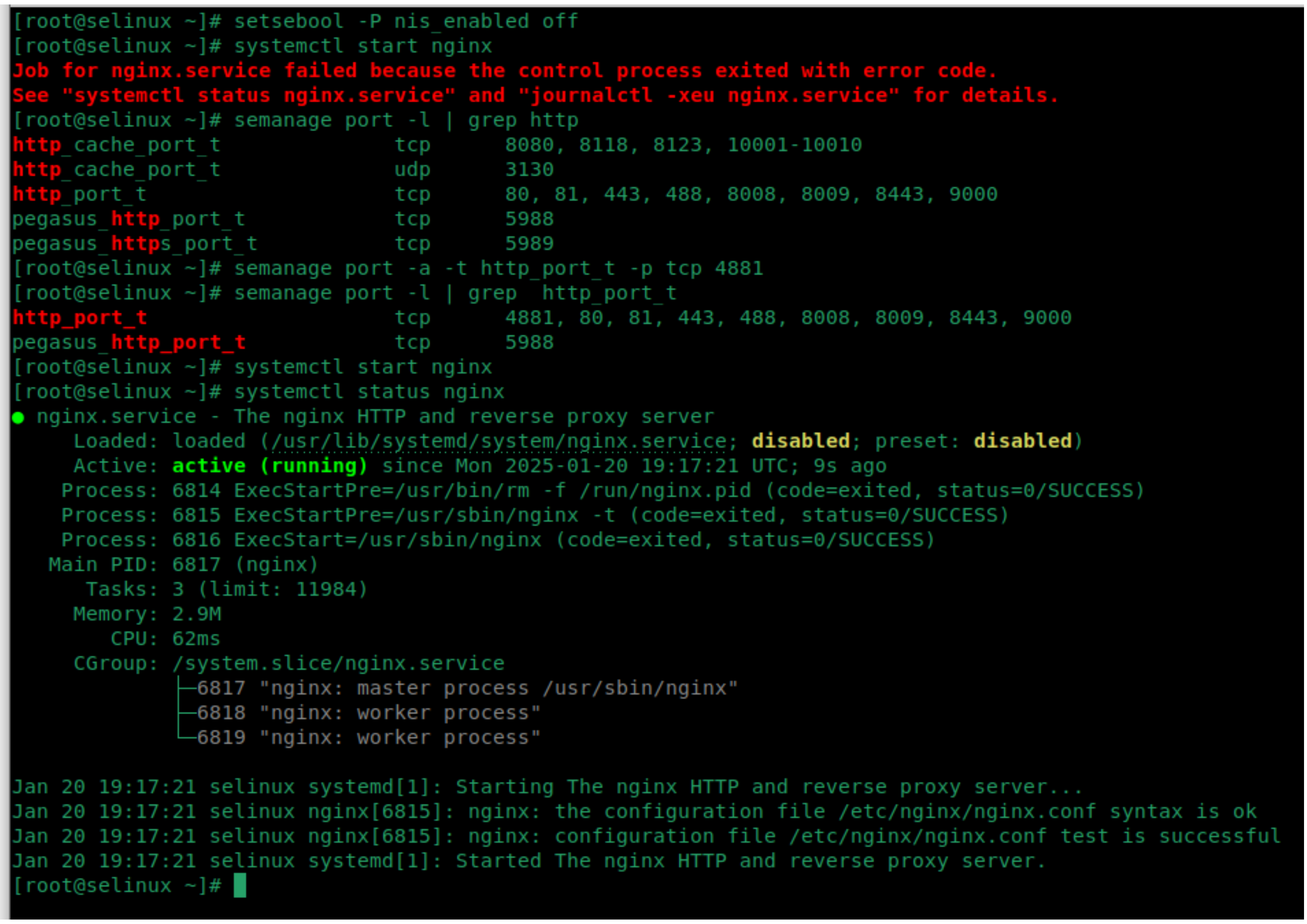
Apache™ is a registered trademark of the Apache Software Foundation in the United States and/or other countries.
NGINX™ is a registered trademark of F5 Networks, Inc..



```
[root@selinux ~]# getsebool -a | grep nis_enabled
nis_enabled --> on
[root@selinux ~]# 
```

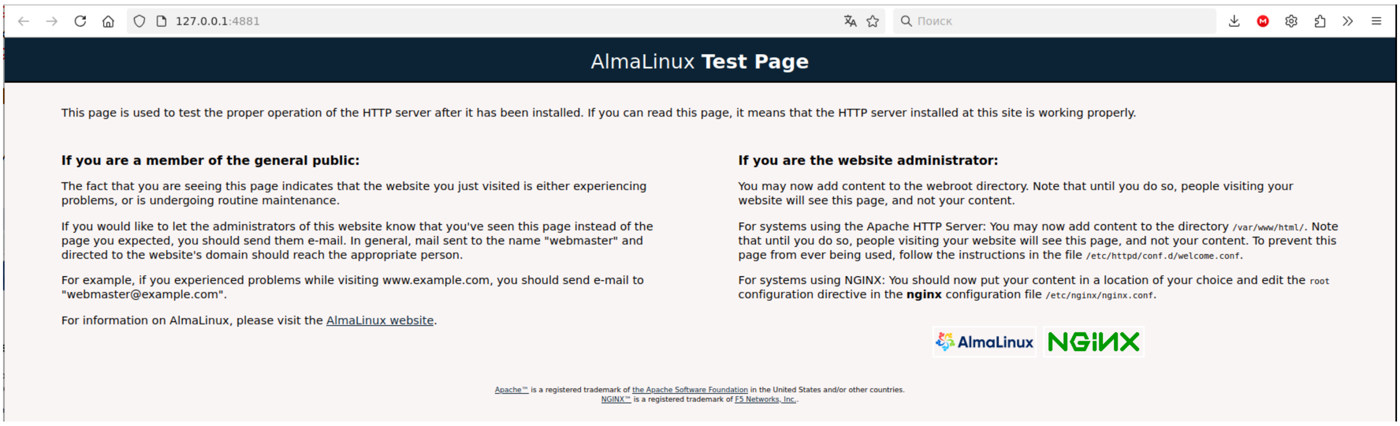
3. Разрешение работы nginx на порту TCP 4881 с помощью добавления нестандартного порта в имеющийся тип командой:

semanage port -a -t http_port_t -p tcp 4881



```
[root@selinux ~]# setsebool -P nis_enabled off
[root@selinux ~]# systemctl start nginx
Job for nginx.service failed because the control process exited with error code.
See "systemctl status nginx.service" and "journalctl -xeu nginx.service" for details.
[root@selinux ~]# semanage port -l | grep http
http_cache_port_t              tcp      8080, 8118, 8123, 10001-10010
http_cache_port_t              udp      3130
http_port_t                    tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t            tcp      5988
pegasus_https_port_t           tcp      5989
[root@selinux ~]# semanage port -a -t http_port_t -p tcp 4881
[root@selinux ~]# semanage port -l | grep  http_port_t
http_port_t                    tcp      4881, 80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t            tcp      5988
[root@selinux ~]# systemctl start nginx
[root@selinux ~]# systemctl status nginx
● nginx.service - The nginx HTTP and reverse proxy server
     Loaded: loaded (/usr/lib/systemd/system/nginx.service; disabled; preset: disabled)
     Active: active (running) since Mon 2025-01-20 19:17:21 UTC; 9s ago
    Process: 6814 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=0/SUCCESS)
    Process: 6815 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=0/SUCCESS)
    Process: 6816 ExecStart=/usr/sbin/nginx (code=exited, status=0/SUCCESS)
   Main PID: 6817 (nginx)
      Tasks: 3 (limit: 11984)
     Memory: 2.9M
        CPU: 62ms
     CGroup: /system.slice/nginx.service
             ├─6817 "nginx: master process /usr/sbin/nginx"
             ├─6818 "nginx: worker process"
             └─6819 "nginx: worker process"

Jan 20 19:17:21 selinux systemd[1]: Starting The nginx HTTP and reverse proxy server...
Jan 20 19:17:21 selinux nginx[6815]: nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
Jan 20 19:17:21 selinux nginx[6815]: nginx: configuration file /etc/nginx/nginx.conf test is successful
Jan 20 19:17:21 selinux systemd[1]: Started The nginx HTTP and reverse proxy server.
[root@selinux ~]# 
```

4. Проверка работы nginx



AlmaLinux **Test Page**

This page is used to test the proper operation of the HTTP server after it has been installed. If you can read this page, it means that the HTTP server installed at this site is working properly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

For information on AlmaLinux, please visit the AlmaLinux website.

If you are the website administrator:

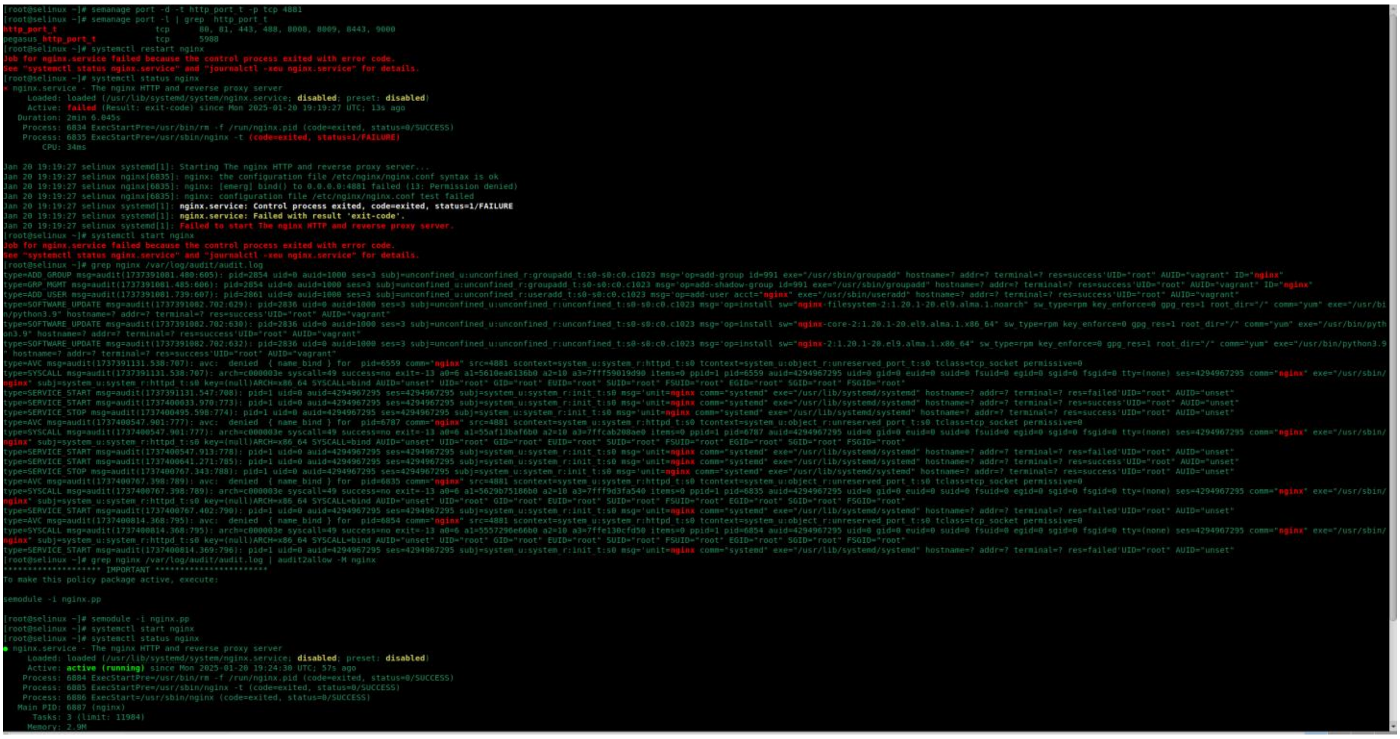
You may now add content to the webroot directory. Note that until you do so, people visiting your website will see this page, and not your content.

For systems using the Apache HTTP Server: You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

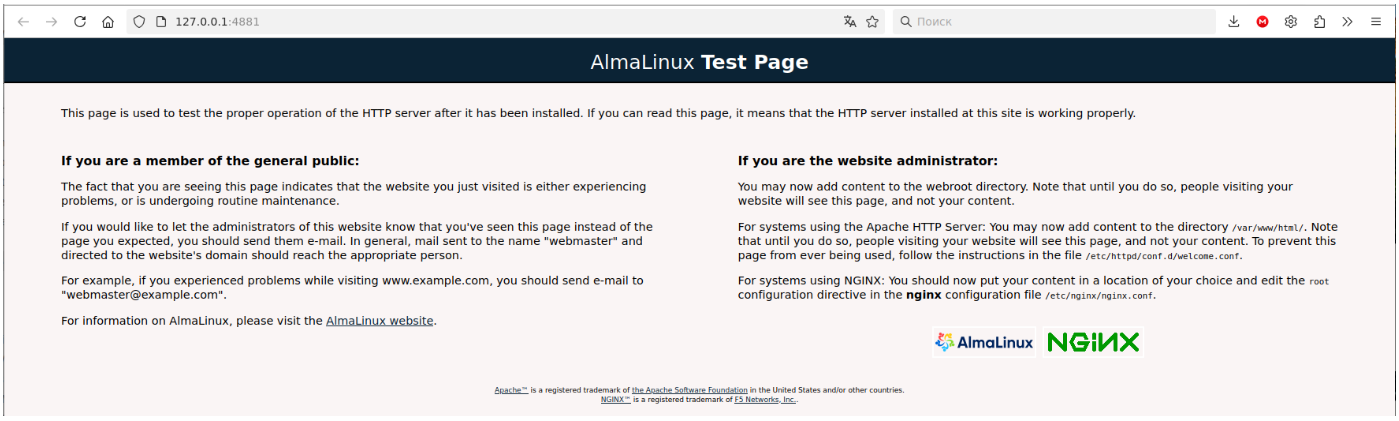
For systems using NGINX: You should now put your content in a location of your choice and edit the `root` configuration directive in the **nginx** configuration file `/etc/nginx/nginx.conf`.

Apache™ is a registered trademark of the Apache Software Foundation in the United States and/or other countries.
NGINX™ is a registered trademark of F5 Networks, Inc..

5. Разрешение в SELinux работу nginx на порту TCP 4881 с помощью формирования и установки модуля SELinux.



```
[root@selinux ~]# semanage port -d -t http_port_t -p tcp 4881
[root@selinux ~]# semanage port -l | grep  http_port_t
http_port_t                    tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t            tcp      5988
[root@selinux ~]# systemctl restart nginx
Job for nginx.service failed because the control process exited with error code.
See "systemctl status nginx.service" and "journalctl -xeu nginx.service" for details.
[root@selinux ~]# systemctl status nginx
× nginx.service - The nginx HTTP and reverse proxy server
     Loaded: loaded (/usr/lib/systemd/system/nginx.service; disabled; preset: disabled)
     Active: failed (Result: exit-code) since Mon 2025-01-20 19:19:27 UTC; 13s ago
   Duration: 2min 6.045s
    Process: 6834 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=0/SUCCESS)
    Process: 6835 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=1/FAILURE)
        CPU: 34ms

Jan 20 19:19:27 selinux systemd[1]: Starting The nginx HTTP and reverse proxy server...
Jan 20 19:19:27 selinux nginx[6835]: nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
Jan 20 19:19:27 selinux nginx[6835]: nginx: [emerg] bind() to 0.0.0.0:4881 failed (13: Permission denied)
Jan 20 19:19:27 selinux nginx[6835]: nginx: configuration file /etc/nginx/nginx.conf test failed
Jan 20 19:19:27 selinux systemd[1]: nginx.service: Control process exited, code=exited, status=1/FAILURE
Jan 20 19:19:27 selinux systemd[1]: nginx.service: Failed with result 'exit-code'.
Jan 20 19:19:27 selinux systemd[1]: Failed to start The nginx HTTP and reverse proxy server.
[root@selinux ~]# systemctl start nginx
Job for nginx.service failed because the control process exited with error code.
See "systemctl status nginx.service" and "journalctl -xeu nginx.service" for details.
[root@selinux ~]# grep nginx /var/log/audit/audit.log
type=ADD_GROUP msg=audit(1737391081.480:605): pid=2854 uid=0 auid=1000 ses=3 subj=unconfined_u:unconfined_r:groupadd_t:s0-s0:c0.c1023 msg='op=add-group id=991 exe="/usr/sbin/groupadd" hostname=? addr=? terminal=? res=success'UID="root" AUID="vagrant" ID="nginx"
type=GRP_MGMT msg=audit(1737391081.485:606): pid=2854 uid=0 auid=1000 ses=3 subj=unconfined_u:unconfined_r:groupadd_t:s0-s0:c0.c1023 msg='op=add-shadow-group id=991 exe="/usr/sbin/groupadd" hostname=? addr=? terminal=? res=success'UID="root" AUID="vagrant" ID="nginx"
type=ADD_USER msg=audit(1737391081.739:607): pid=2861 uid=0 auid=1000 ses=3 subj=unconfined_u:unconfined_r:useradd_t:s0-s0:c0.c1023 msg='op=add-user acct="nginx" exe="/usr/sbin/useradd" hostname=? addr=? terminal=? res=success'UID="root" AUID="vagrant"
type=SOFTWARE_UPDATE msg=audit(1737391082.702:629): pid=2836 uid=0 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=install sw="nginx-filesystem-2:1.20.1-20.el9.alma.1.noarch" sw_type=rpm key_enforce=0 gpg_res=1 root_dir="/" comm="yum" exe="/usr/bi
n/python3.9" hostname=? addr=? terminal=? res=success'UID="root" AUID="vagrant"
type=SOFTWARE_UPDATE msg=audit(1737391082.702:630): pid=2836 uid=0 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=install sw="nginx-core-2:1.20.1-20.el9.alma.1.x86_64" sw_type=rpm key_enforce=0 gpg_res=1 root_dir="/" comm="yum" exe="/usr/bin/pyth
on3.9" hostname=? addr=? terminal=? res=success'UID="root" AUID="vagrant"
type=SOFTWARE_UPDATE msg=audit(1737391082.702:632): pid=2836 uid=0 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=install sw="nginx-2:1.20.1-20.el9.alma.1.x86_64" sw_type=rpm key_enforce=0 gpg_res=1 root_dir="/" comm="yum" exe="/usr/bin/python3.9
" hostname=? addr=? terminal=? res=success'UID="root" AUID="vagrant"
type=AVC msg=audit(1737391131.538:707): avc:  denied  { name_bind } for  pid=6559 comm="nginx" src=4881 scontext=system_u:system_r:httpd_t:s0 tcontext=system_u:object_r:unreserved_port_t:s0 tclass=tcp_socket permissive=0
type=SYSCALL msg=audit(1737391131.538:707): arch=c000003e syscall=49 success=no exit=-13 a0=6 a1=5610ea6136b0 a2=10 a3=7fff59019d90 items=0 ppid=1 pid=6559 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="nginx" exe="/usr/sbin/
nginx" subj=system_u:system_r:httpd_t:s0 key=(null)ARCH=x86_64 SYSCALL=bind AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=SERVICE_START msg=audit(1737391131.547:708): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=nginx comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=failed'UID="root" AUID="unset"
type=SERVICE_START msg=audit(1737400033.970:773): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=nginx comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1737400495.598:774): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=nginx comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=AVC msg=audit(1737400547.901:777): avc:  denied  { name_bind } for  pid=6787 comm="nginx" src=4881 scontext=system_u:system_r:httpd_t:s0 tcontext=system_u:object_r:unreserved_port_t:s0 tclass=tcp_socket permissive=0
type=SYSCALL msg=audit(1737400547.901:777): arch=c000003e syscall=49 success=no exit=-13 a0=6 a1=55af13baf6b0 a2=10 a3=7ffcab208ae0 items=0 ppid=1 pid=6787 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="nginx" exe="/usr/sbin/
nginx" subj=system_u:system_r:httpd_t:s0 key=(null)ARCH=x86_64 SYSCALL=bind AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=SERVICE_START msg=audit(1737400547.913:778): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=nginx comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=failed'UID="root" AUID="unset"
type=SERVICE_START msg=audit(1737400641.271:785): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=nginx comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1737400767.343:788): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=nginx comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=AVC msg=audit(1737400767.398:789): avc:  denied  { name_bind } for  pid=6835 comm="nginx" src=4881 scontext=system_u:system_r:httpd_t:s0 tcontext=system_u:object_r:unreserved_port_t:s0 tclass=tcp_socket permissive=0
type=SYSCALL msg=audit(1737400767.398:789): arch=c000003e syscall=49 success=no exit=-13 a0=6 a1=5629b75186b0 a2=10 a3=7fff9d3fa540 items=0 ppid=1 pid=6835 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="nginx" exe="/usr/sbin/
nginx" subj=system_u:system_r:httpd_t:s0 key=(null)ARCH=x86_64 SYSCALL=bind AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=SERVICE_START msg=audit(1737400767.402:790): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=nginx comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=failed'UID="root" AUID="unset"
type=AVC msg=audit(1737400814.368:795): avc:  denied  { name_bind } for  pid=6854 comm="nginx" src=4881 scontext=system_u:system_r:httpd_t:s0 tcontext=system_u:object_r:unreserved_port_t:s0 tclass=tcp_socket permissive=0
type=SYSCALL msg=audit(1737400814.368:795): arch=c000003e syscall=49 success=no exit=-13 a0=6 a1=5557296e66b0 a2=10 a3=7ffe130cfd50 items=0 ppid=1 pid=6854 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="nginx" exe="/usr/sbin/
nginx" subj=system_u:system_r:httpd_t:s0 key=(null)ARCH=x86_64 SYSCALL=bind AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=SERVICE_START msg=audit(1737400814.369:796): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=nginx comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=failed'UID="root" AUID="unset"
[root@selinux ~]# grep nginx /var/log/audit/audit.log | audit2allow -M nginx
******************** IMPORTANT ***********************
To make this policy package active, execute:

semodule -i nginx.pp

[root@selinux ~]# semodule -i nginx.pp
[root@selinux ~]# systemctl start nginx
[root@selinux ~]# systemctl status nginx
● nginx.service - The nginx HTTP and reverse proxy server
     Loaded: loaded (/usr/lib/systemd/system/nginx.service; disabled; preset: disabled)
     Active: active (running) since Mon 2025-01-20 19:24:30 UTC; 57s ago
    Process: 6884 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=0/SUCCESS)
    Process: 6885 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=0/SUCCESS)
    Process: 6886 ExecStart=/usr/sbin/nginx (code=exited, status=0/SUCCESS)
   Main PID: 6887 (nginx)
      Tasks: 3 (limit: 11984)
     Memory: 2.9M
```



AlmaLinux **Test Page**

This page is used to test the proper operation of the HTTP server after it has been installed. If you can read this page, it means that the HTTP server installed at this site is working properly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

For information on AlmaLinux, please visit the AlmaLinux website.

If you are the website administrator:

You may now add content to the webroot directory. Note that until you do so, people visiting your website will see this page, and not your content.

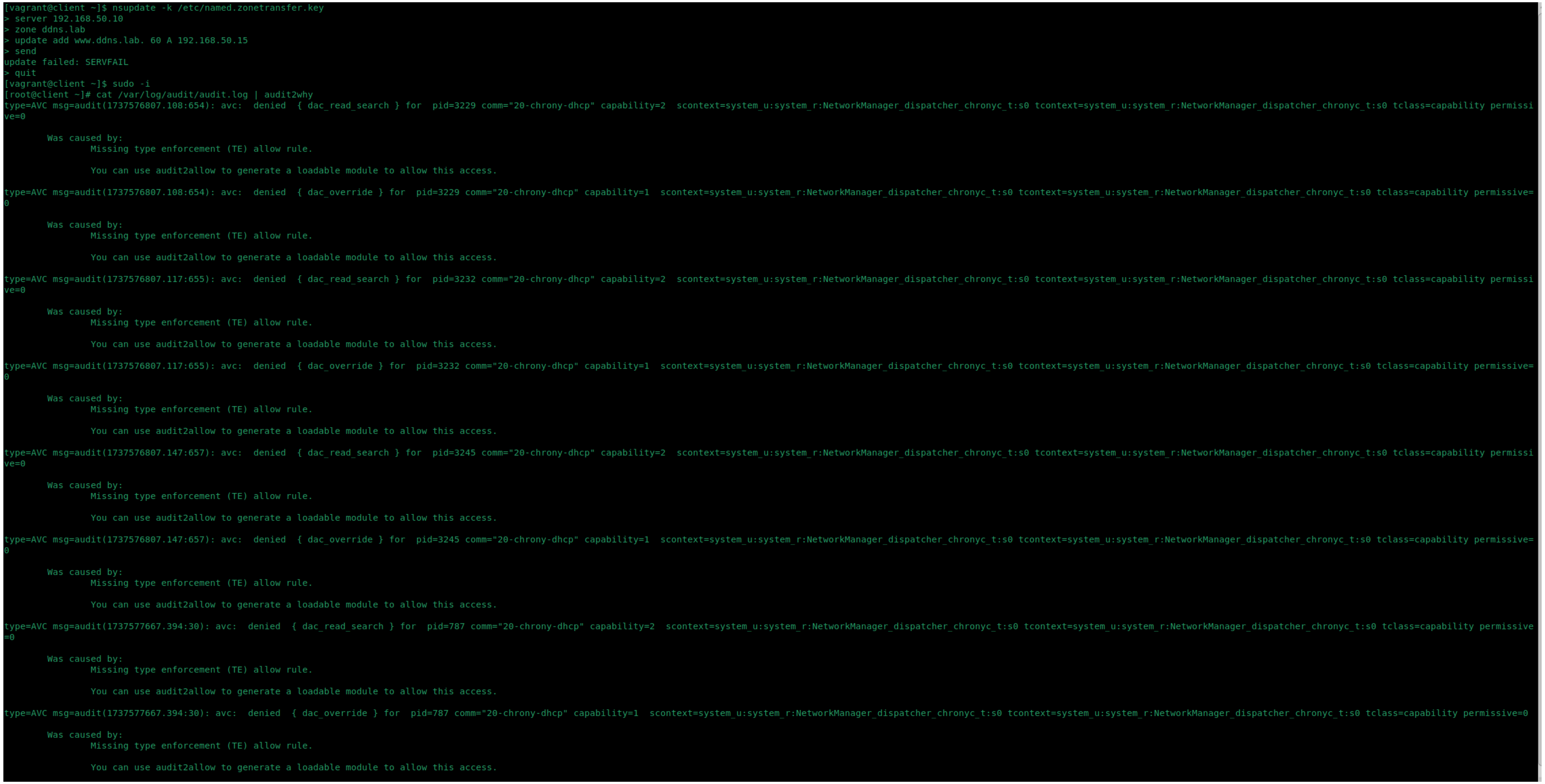
For systems using the Apache HTTP Server: You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

For systems using NGINX: You should now put your content in a location of your choice and edit the `root` configuration directive in the **nginx** configuration file `/etc/nginx/nginx.conf`.

Apache™ is a registered trademark of the Apache Software Foundation in the United States and/or other countries.
NGINX™ is a registered trademark of F5 Networks, Inc..

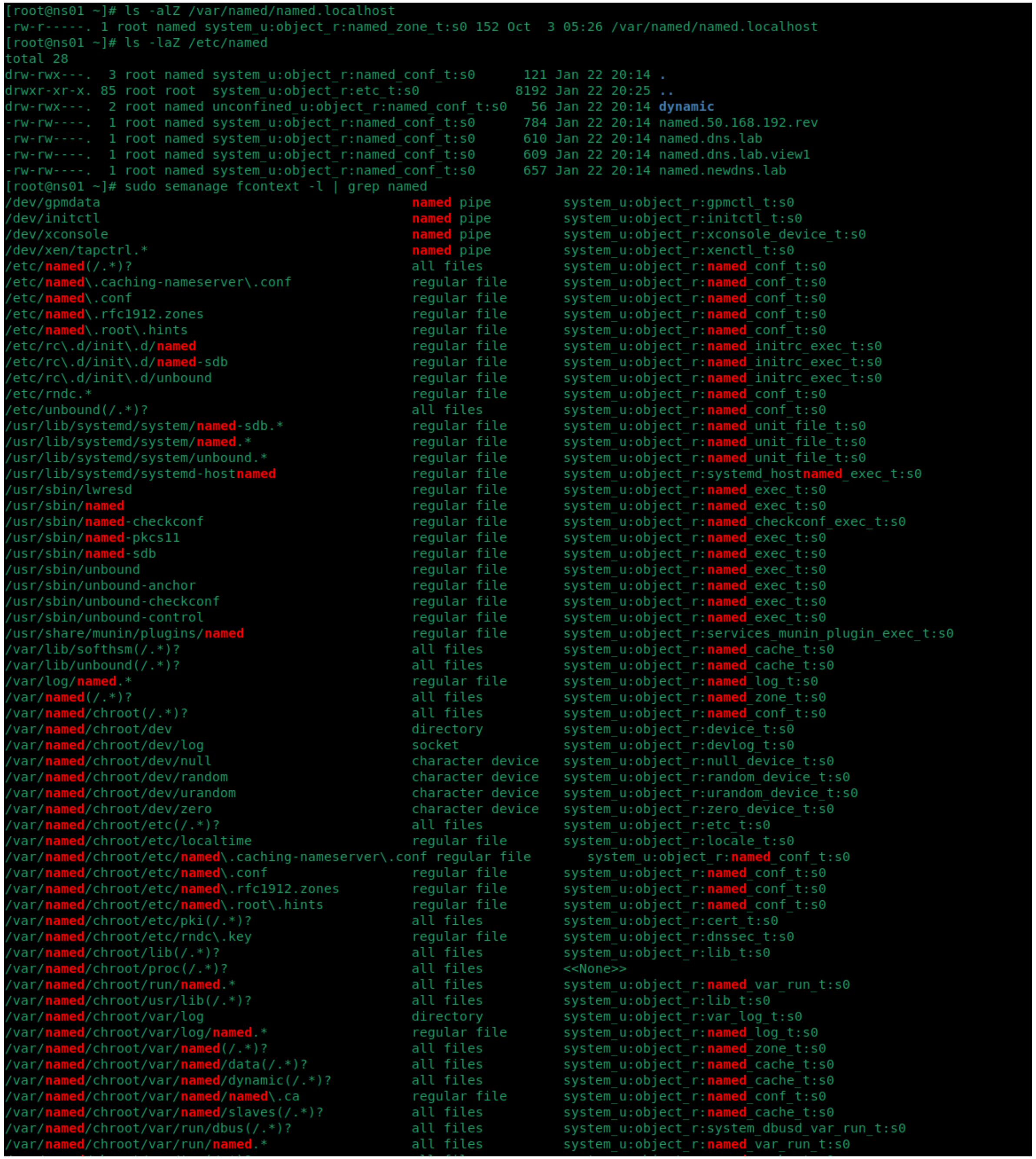
- Часть 2. Обеспечение работоспособности приложения при включенном SELinux

1. Ошибка при изменении записи в зоне на клиенте DNS:



```
[vagrant@client ~]$ nsupdate -k /etc/named.zonetransfer.key
> server 192.168.50.10
> zone ddns.lab
> update add www.ddns.lab. 60 A 192.168.50.15
> send
update failed: SERVFAIL
> quit
[vagrant@client ~]$ sudo -i
[root@client ~]# cat /var/log/audit/audit.log | audit2why
type=AVC msg=audit(1737576807.108:654): avc:  denied  { dac_read_search } for  pid=3229 comm="20-chrony-dhcp" capability=2  scontext=system_u:system_r:NetworkManager_dispatcher_chronyc_t:s0 tcontext=system_u:system_r:NetworkManager_dispatcher_chronyc_t:s0 tclass=capability permissi
ve=0

        Was caused by:
                Missing type enforcement (TE) allow rule.

                You can use audit2allow to generate a loadable module to allow this access.

type=AVC msg=audit(1737576807.108:654): avc:  denied  { dac_override } for  pid=3229 comm="20-chrony-dhcp" capability=1  scontext=system_u:system_r:NetworkManager_dispatcher_chronyc_t:s0 tcontext=system_u:system_r:NetworkManager_dispatcher_chronyc_t:s0 tclass=capability permissive=
0

        Was caused by:
                Missing type enforcement (TE) allow rule.

                You can use audit2allow to generate a loadable module to allow this access.

type=AVC msg=audit(1737576807.117:655): avc:  denied  { dac_read_search } for  pid=3232 comm="20-chrony-dhcp" capability=2  scontext=system_u:system_r:NetworkManager_dispatcher_chronyc_t:s0 tcontext=system_u:system_r:NetworkManager_dispatcher_chronyc_t:s0 tclass=capability permissi
ve=0

        Was caused by:
                Missing type enforcement (TE) allow rule.

                You can use audit2allow to generate a loadable module to allow this access.

type=AVC msg=audit(1737576807.117:655): avc:  denied  { dac_override } for  pid=3232 comm="20-chrony-dhcp" capability=1  scontext=system_u:system_r:NetworkManager_dispatcher_chronyc_t:s0 tcontext=system_u:system_r:NetworkManager_dispatcher_chronyc_t:s0 tclass=capability permissive=
0

        Was caused by:
                Missing type enforcement (TE) allow rule.

                You can use audit2allow to generate a loadable module to allow this access.

type=AVC msg=audit(1737576807.147:657): avc:  denied  { dac_read_search } for  pid=3245 comm="20-chrony-dhcp" capability=2  scontext=system_u:system_r:NetworkManager_dispatcher_chronyc_t:s0 tcontext=system_u:system_r:NetworkManager_dispatcher_chronyc_t:s0 tclass=capability permissi
ve=0

        Was caused by:
                Missing type enforcement (TE) allow rule.

                You can use audit2allow to generate a loadable module to allow this access.

type=AVC msg=audit(1737576807.147:657): avc:  denied  { dac_override } for  pid=3245 comm="20-chrony-dhcp" capability=1  scontext=system_u:system_r:NetworkManager_dispatcher_chronyc_t:s0 tcontext=system_u:system_r:NetworkManager_dispatcher_chronyc_t:s0 tclass=capability permissive=
0

        Was caused by:
                Missing type enforcement (TE) allow rule.

                You can use audit2allow to generate a loadable module to allow this access.

type=AVC msg=audit(1737577667.394:30): avc:  denied  { dac_read_search } for  pid=787 comm="20-chrony-dhcp" capability=2  scontext=system_u:system_r:NetworkManager_dispatcher_chronyc_t:s0 tcontext=system_u:system_r:NetworkManager_dispatcher_chronyc_t:s0 tclass=capability permissive
=0

        Was caused by:
                Missing type enforcement (TE) allow rule.

                You can use audit2allow to generate a loadable module to allow this access.

type=AVC msg=audit(1737577667.394:30): avc:  denied  { dac_override } for  pid=787 comm="20-chrony-dhcp" capability=1  scontext=system_u:system_r:NetworkManager_dispatcher_chronyc_t:s0 tcontext=system_u:system_r:NetworkManager_dispatcher_chronyc_t:s0 tclass=capability permissive=0

        Was caused by:
                Missing type enforcement (TE) allow rule.

                You can use audit2allow to generate a loadable module to allow this access.
```

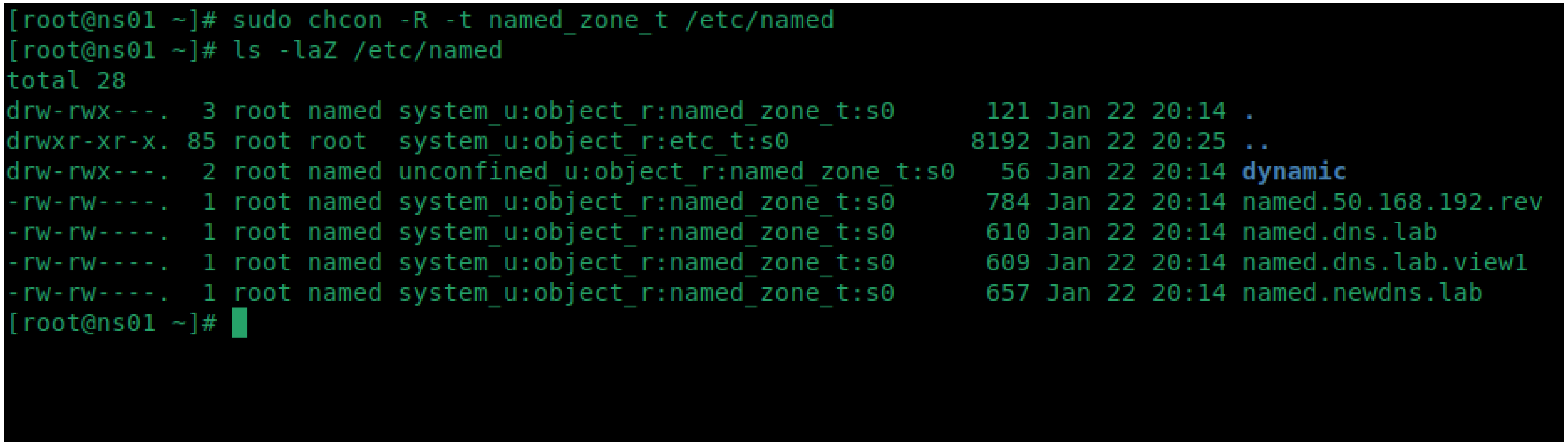
2. Логи SELinux на сервере:



```
[root@ns01 ~]# ls -alZ /var/named/named.localhost
-rw-r-----. 1 root named system_u:object_r:named_zone_t:s0 152 Oct  3 05:26 /var/named/named.localhost
[root@ns01 ~]# ls -laZ /etc/named
total 28
drw-rwx---.  3 root named system_u:object_r:named_conf_t:s0      121 Jan 22 20:14 .
drwxr-xr-x. 85 root root  system_u:object_r:etc_t:s0           8192 Jan 22 20:25 ..
drw-rwx---.  2 root named unconfined_u:object_r:named_conf_t:s0   56 Jan 22 20:14 dynamic
-rw-rw----.  1 root named system_u:object_r:named_conf_t:s0      784 Jan 22 20:14 named.50.168.192.rev
-rw-rw----.  1 root named system_u:object_r:named_conf_t:s0      610 Jan 22 20:14 named.dns.lab
-rw-rw----.  1 root named system_u:object_r:named_conf_t:s0      609 Jan 22 20:14 named.dns.lab.view1
-rw-rw----.  1 root named system_u:object_r:named_conf_t:s0      657 Jan 22 20:14 named.newdns.lab
[root@ns01 ~]# sudo semanage fcontext -l | grep named
/dev/gpmdata                                       named pipe         system_u:object_r:gpmctl_t:s0
/dev/initctl                                       named pipe         system_u:object_r:initctl_t:s0
/dev/xconsole                                      named pipe         system_u:object_r:xconsole_device_t:s0
/dev/xen/tapctrl.*                                 named pipe         system_u:object_r:xenctl_t:s0
/etc/named(/.*)?                                   all files          system_u:object_r:named_conf_t:s0
/etc/named\.caching-nameserver\.conf               regular file       system_u:object_r:named_conf_t:s0
/etc/named\.conf                                   regular file       system_u:object_r:named_conf_t:s0
/etc/named\.rfc1912.zones                          regular file       system_u:object_r:named_conf_t:s0
/etc/named\.root\.hints                            regular file       system_u:object_r:named_conf_t:s0
/etc/rc\.d/init\.d/named                           regular file       system_u:object_r:named_initrc_exec_t:s0
/etc/rc\.d/init\.d/named-sdb                       regular file       system_u:object_r:named_initrc_exec_t:s0
/etc/rc\.d/init\.d/unbound                         regular file       system_u:object_r:named_initrc_exec_t:s0
/etc/rndc.*                                        regular file       system_u:object_r:named_conf_t:s0
/etc/unbound(/.*)?                                 all files          system_u:object_r:named_conf_t:s0
/usr/lib/systemd/system/named-sdb.*                regular file       system_u:object_r:named_unit_file_t:s0
/usr/lib/systemd/system/named.*                    regular file       system_u:object_r:named_unit_file_t:s0
/usr/lib/systemd/system/unbound.*                  regular file       system_u:object_r:named_unit_file_t:s0
/usr/lib/systemd/systemd-hostnamed                 regular file       system_u:object_r:systemd_hostnamed_exec_t:s0
/usr/sbin/lwresd                                   regular file       system_u:object_r:named_exec_t:s0
/usr/sbin/named                                    regular file       system_u:object_r:named_exec_t:s0
/usr/sbin/named-checkconf                          regular file       system_u:object_r:named_checkconf_exec_t:s0
/usr/sbin/named-pkcs11                             regular file       system_u:object_r:named_exec_t:s0
/usr/sbin/named-sdb                                regular file       system_u:object_r:named_exec_t:s0
/usr/sbin/unbound                                  regular file       system_u:object_r:named_exec_t:s0
/usr/sbin/unbound-anchor                           regular file       system_u:object_r:named_exec_t:s0
/usr/sbin/unbound-checkconf                        regular file       system_u:object_r:named_exec_t:s0
/usr/sbin/unbound-control                          regular file       system_u:object_r:named_exec_t:s0
/usr/share/munin/plugins/named                     regular file       system_u:object_r:services_munin_plugin_exec_t:s0
/var/lib/softhsm(/.*)?                             all files          system_u:object_r:named_cache_t:s0
/var/lib/unbound(/.*)?                             all files          system_u:object_r:named_cache_t:s0
/var/log/named.*                                   regular file       system_u:object_r:named_log_t:s0
/var/named(/.*)?                                   all files          system_u:object_r:named_zone_t:s0
/var/named/chroot(/.*)?                            all files          system_u:object_r:named_conf_t:s0
/var/named/chroot/dev                              directory          system_u:object_r:device_t:s0
/var/named/chroot/dev/log                          socket             system_u:object_r:devlog_t:s0
/var/named/chroot/dev/null                         character device   system_u:object_r:null_device_t:s0
/var/named/chroot/dev/random                       character device   system_u:object_r:random_device_t:s0
/var/named/chroot/dev/urandom                      character device   system_u:object_r:urandom_device_t:s0
/var/named/chroot/dev/zero                         character device   system_u:object_r:zero_device_t:s0
/var/named/chroot/etc(/.*)?                        all files          system_u:object_r:etc_t:s0
/var/named/chroot/etc/localtime                    regular file       system_u:object_r:locale_t:s0
/var/named/chroot/etc/named\.caching-nameserver\.conf regular file       system_u:object_r:named_conf_t:s0
/var/named/chroot/etc/named\.conf                  regular file       system_u:object_r:named_conf_t:s0
/var/named/chroot/etc/named\.rfc1912.zones         regular file       system_u:object_r:named_conf_t:s0
/var/named/chroot/etc/named\.root\.hints           regular file       system_u:object_r:named_conf_t:s0
/var/named/chroot/etc/pki(/.*)?                    all files          system_u:object_r:cert_t:s0
/var/named/chroot/etc/rndc\.key                    regular file       system_u:object_r:dnssec_t:s0
/var/named/chroot/lib(/.*)?                        all files          system_u:object_r:lib_t:s0
/var/named/chroot/proc(/.*)?                       all files          <<None>>
/var/named/chroot/run/named.*                      all files          system_u:object_r:named_var_run_t:s0
/var/named/chroot/usr/lib(/.*)?                    all files          system_u:object_r:lib_t:s0
/var/named/chroot/var/log                          directory          system_u:object_r:var_log_t:s0
/var/named/chroot/var/log/named.*                  regular file       system_u:object_r:named_log_t:s0
/var/named/chroot/var/named(/.*)?                  all files          system_u:object_r:named_zone_t:s0
/var/named/chroot/var/named/data(/.*)?             all files          system_u:object_r:named_cache_t:s0
/var/named/chroot/var/named/dynamic(/.*)?          all files          system_u:object_r:named_cache_t:s0
/var/named/chroot/var/named/named\.ca              regular file       system_u:object_r:named_conf_t:s0
/var/named/chroot/var/named/slaves(/.*)?           all files          system_u:object_r:named_cache_t:s0
/var/named/chroot/var/run/dbus(/.*)?               all files          system_u:object_r:system_dbusd_var_run_t:s0
/var/named/chroot/var/run/named.*                  all files          system_u:object_r:named_var_run_t:s0
```

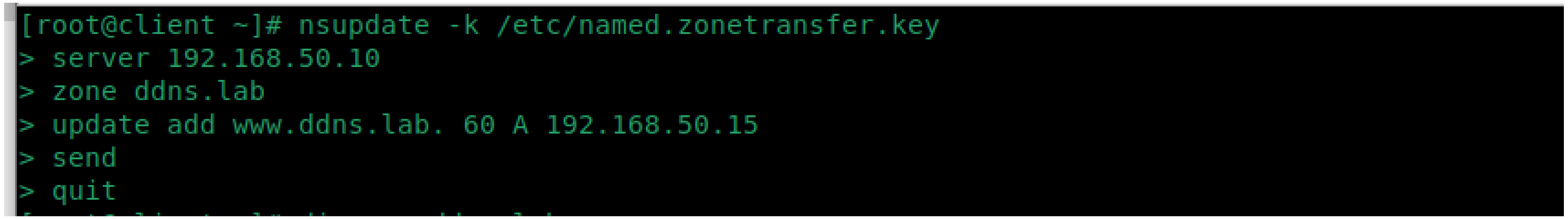
3. Изменение типа контекста безопасности для каталога /etc/named командой:

sudo chcon -R -t named_zone_t /etc/named



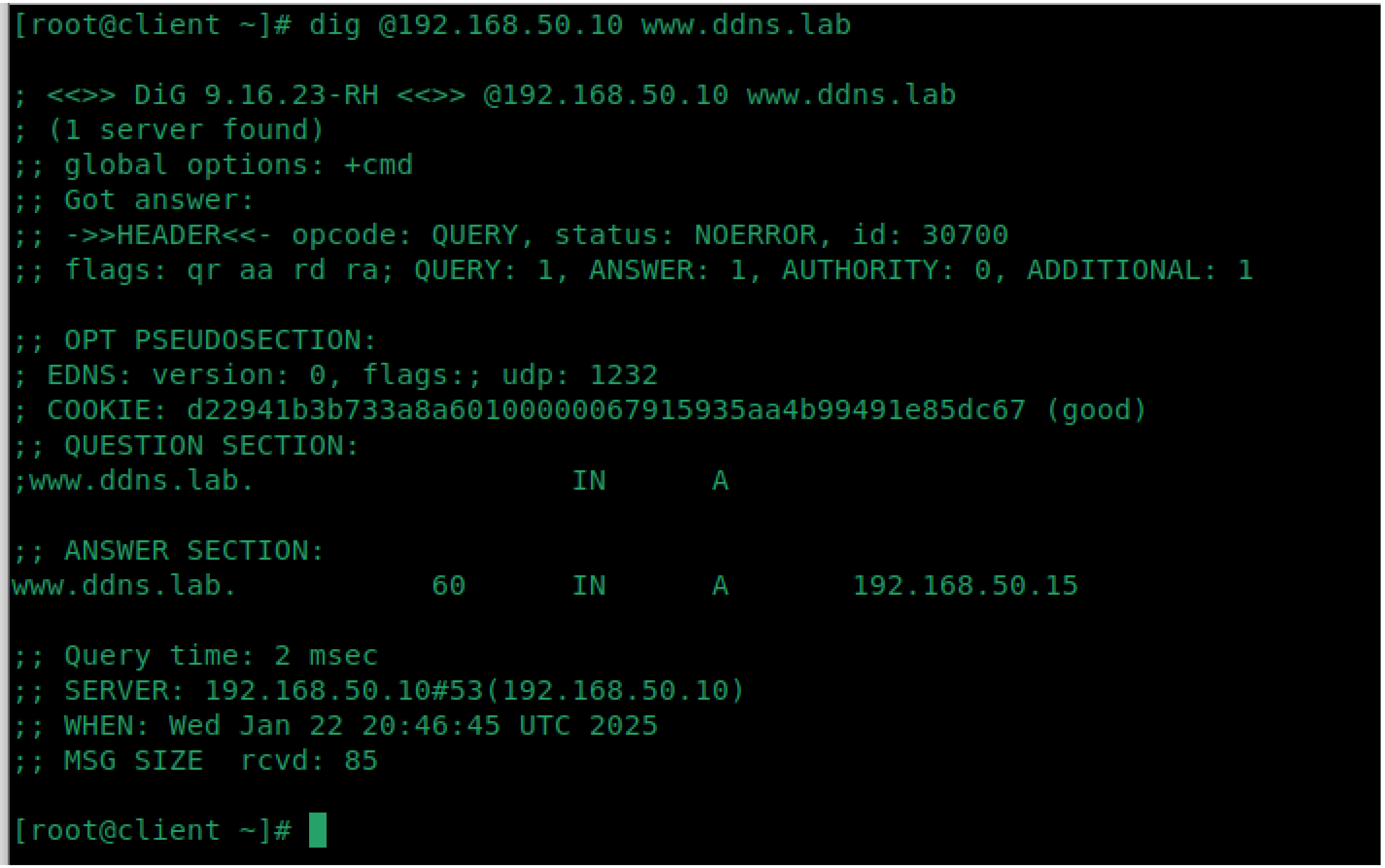
```
[root@ns01 ~]# sudo chcon -R -t named_zone_t /etc/named
[root@ns01 ~]# ls -laZ /etc/named
total 28
drw-rwx---.  3 root named system_u:object_r:named_zone_t:s0      121 Jan 22 20:14 .
drwxr-xr-x. 85 root root  system_u:object_r:etc_t:s0            8192 Jan 22 20:25 ..
drw-rwx---.  2 root named unconfined_u:object_r:named_zone_t:s0   56 Jan 22 20:14 dynamic
-rw-rw----.  1 root named system_u:object_r:named_zone_t:s0      784 Jan 22 20:14 named.50.168.192.rev
-rw-rw----.  1 root named system_u:object_r:named_zone_t:s0      610 Jan 22 20:14 named.dns.lab
-rw-rw----.  1 root named system_u:object_r:named_zone_t:s0      609 Jan 22 20:14 named.dns.lab.view1
-rw-rw----.  1 root named system_u:object_r:named_zone_t:s0      657 Jan 22 20:14 named.newdns.lab
[root@ns01 ~]# 
```

4. Проверка со стороны клиента:



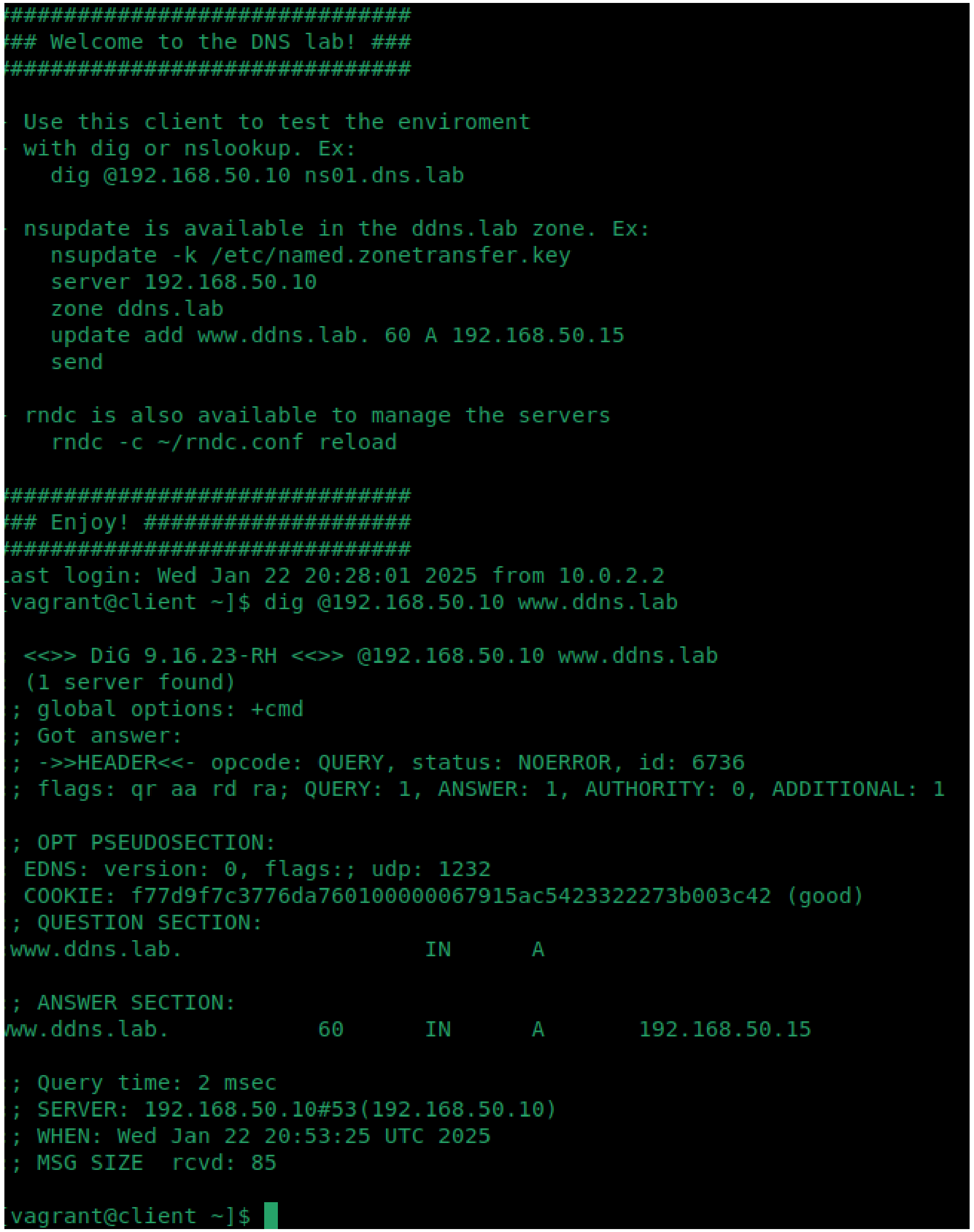
```
[root@client ~]# nsupdate -k /etc/named.zonetransfer.key
> server 192.168.50.10
> zone ddns.lab
> update add www.ddns.lab. 60 A 192.168.50.15
> send
> quit
```

5. Проверка командой dig



```
[root@client ~]# dig @192.168.50.10 www.ddns.lab

; <<>> DiG 9.16.23-RH <<>> @192.168.50.10 www.ddns.lab
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30700
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d22941b3b733a8a60100000067915935aa4b99491e85dc67 (good)
;; QUESTION SECTION:
;www.ddns.lab.                  IN      A

;; ANSWER SECTION:
www.ddns.lab.           60      IN      A       192.168.50.15

;; Query time: 2 msec
;; SERVER: 192.168.50.10#53(192.168.50.10)
;; WHEN: Wed Jan 22 20:46:45 UTC 2025
;; MSG SIZE  rcvd: 85

[root@client ~]# 
```

6. И после перезагрузки:



```
###############################
### Welcome to the DNS lab! ###
###############################

- Use this client to test the enviroment
- with dig or nslookup. Ex:
    dig @192.168.50.10 ns01.dns.lab

- nsupdate is available in the ddns.lab zone. Ex:
    nsupdate -k /etc/named.zonetransfer.key
    server 192.168.50.10
    zone ddns.lab
    update add www.ddns.lab. 60 A 192.168.50.15
    send

- rndc is also available to manage the servers
    rndc -c ~/rndc.conf reload

###############################
### Enjoy! ####################
###############################
ast login: Wed Jan 22 20:28:01 2025 from 10.0.2.2
[vagrant@client ~]$ dig @192.168.50.10 www.ddns.lab

; <<>> DiG 9.16.23-RH <<>> @192.168.50.10 www.ddns.lab
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6736
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: f77d9f7c3776da760100000067915ac5423322273b003c42 (good)
;; QUESTION SECTION:
;www.ddns.lab.                  IN      A

;; ANSWER SECTION:
ww.ddns.lab.            60      IN      A       192.168.50.15

;; Query time: 2 msec
;; SERVER: 192.168.50.10#53(192.168.50.10)
;; WHEN: Wed Jan 22 20:53:25 UTC 2025
;; MSG SIZE  rcvd: 85

[vagrant@client ~]$
```