

Отчёт о лабораторной работе

Лабораторная работа 9. Управление SELinux

Баранов Никита Дмитриевич

Содержание

1. Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

2. Задание

1. Продемонстрируйте навыки по управлению режимами SELinux (см. раздел 9.4.1).
2. Продемонстрируйте навыки по восстановлению контекста безопасности SELinux (см. раздел 9.4.2).
3. Настройте контекст безопасности для нестандартного расположения файлов вебслужбы (см. раздел 9.4.3).
4. Продемонстрируйте навыки работы с переключателями SELinux (см. раздел 9.4.4).

3. Выполнение лабораторной работы

3.1 Работа с режимами SELinux

Получаем полномочия администратора и просматриваем текущую информацию о состоянии SELinux (рис. [fig:001?]).

```
Activities Terminal Sep 8 19:47 en
root@ndbaranov:~
[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# sestatus -v
SELinux status: enabled
SELinuxfs mount: /sys/fs/selinux
SELinux root directory: /etc/selinux
Loaded policy name: targeted
Current mode: enforcing
Mode from config file: enforcing
Policy MLS status: enabled
Policy deny_unknown status: allowed
Memory protection checking: actual (secure)
Max kernel policy version: 33

Process contexts:
Current context: unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
Init context: system_u:system_r:init_t:s0
/usr/sbin/sshd system_u:system_r:sshd_t:s0-s0:c0.c1023

File contexts:
Controlling terminal: unconfined_u:object_r:user_devpts_t:s0
/etc/passwd system_u:object_r:passwd_file_t:s0
/etc/shadow system_u:object_r:shadow_t:s0
/bin/bash system_u:object_r:shell_exec_t:s0
/bin/login system_u:object_r:login_exec_t:s0
/bin/sh system_u:object_r:bin_t:s0 -> system_u:object_r:shell_exec_t:s0
/sbin/agetty system_u:object_r:getty_exec_t:s0
/sbin/init system_u:object_r:bin_t:s0 -> system_u:object_r:init_exec_t:s0
/usr/sbin/sshd system_u:object_r:sshd_exec_t:s0
[root@ndbaranov ~]# getenforce
Enforcing
[root@ndbaranov ~]# setenforce 0
[root@ndbaranov ~]# getenforce
Permissive
[root@ndbaranov ~]# nano /etc/sysconfig/selinux
[root@ndbaranov ~]#
```

Просмотр статуса SELinux

Информация о состоянии SELinux: - SELinux status: enabled - SELinux включен - SELinuxfs mount: /sys/fs/selinux - точка монтирования файловой системы SELinux - SELinux root directory: /etc/selinux - корневой каталог конфигурации SELinux - Loaded policy name: targeted - загружена политика targeted - Current mode: enforcing - текущий режим: принудительный - Mode from config file: enforcing - режим из конфигурационного файла: принудительный - Policy MLS status: enabled - поддержка многоуровневой безопасности включена - Policy deny_unknown status: allowed - политика разрешает неизвестные статусы - Memory protection checking: actual (secure) - проверка защиты памяти: актуальная (безопасная)

Проверяем текущий режим работы SELinux (рис. [fig:001?]).

```
Activities Terminal Sep 8 19:47 en
root@ndbaranov:~

[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# sestatus -v
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:       /etc/selinux
Loaded policy name:            targeted
Current mode:                  enforcing
Mode from config file:        enforcing
Policy MLS status:             enabled
Policy deny_unknown status:    allowed
Memory protection checking:    actual (secure)
Max kernel policy version:    33

Process contexts:
Current context:               unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
Init context:                  system_u:system_r:init_t:s0
/usr/sbin/sshd                 system_u:system_r:sshd_t:s0-s0:c0.c1023

File contexts:
Controlling terminal:         unconfined_u:object_r:user_devpts_t:s0
/etc/passwd                   system_u:object_r:passwd_file_t:s0
/etc/shadow                   system_u:object_r:shadow_t:s0
/bin/bash                     system_u:object_r:shell_exec_t:s0
/bin/login                    system_u:object_r:login_exec_t:s0
/bin/sh                       system_u:object_r:bin_t:s0 -> system_u:object_r:shell_exec_t:s0
/sbin/agetty                  system_u:object_r:getty_exec_t:s0
/sbin/init                    system_u:object_r:bin_t:s0 -> system_u:object_r:init_exec_t:s0
/usr/sbin/sshd                 system_u:object_r:sshd_exec_t:s0

[root@ndbaranov ~]# getenforce
Enforcing
[root@ndbaranov ~]# setenforce 0
[root@ndbaranov ~]# getenforce
Permissive
[root@ndbaranov ~]# nano /etc/sysconfig/selinux
[root@ndbaranov ~]#
```

Проверка режима *getenforce*

Изменяем режим работы на разрешающий (Permissive) и проверяем (рис. [fig:001?]).

```
Activities Terminal Sep 8 19:47 en
root@ndbaranov:~

[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# sestatus -v
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:      /etc/selinux
Loaded policy name:           targeted
Current mode:                 enforcing
Mode from config file:       enforcing
Policy MLS status:           enabled
Policy deny_unknown status:   allowed
Memory protection checking:   actual (secure)
Max kernel policy version:    33

Process contexts:
Current context:              unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
Init context:                 system_u:system_r:init_t:s0
/usr/sbin/sshd                system_u:system_r:sshd_t:s0-s0:c0.c1023

File contexts:
Controlling terminal:         unconfined_u:object_r:user_devpts_t:s0
/etc/passwd                   system_u:object_r:passwd_file_t:s0
/etc/shadow                   system_u:object_r:shadow_t:s0
/bin/bash                     system_u:object_r:shell_exec_t:s0
/bin/login                    system_u:object_r:login_exec_t:s0
/bin/sh                       system_u:object_r:bin_t:s0 -> system_u:object_r:shell_exec_t:s0
/sbin/agetty                  system_u:object_r:getty_exec_t:s0
/sbin/init                    system_u:object_r:bin_t:s0 -> system_u:object_r:init_exec_t:s0
/usr/sbin/sshd                system_u:object_r:sshd_exec_t:s0
[root@ndbaranov ~]# getenforce
Enforcing
[root@ndbaranov ~]# setenforce 0
[root@ndbaranov ~]# getenforce
Permissive
[root@ndbaranov ~]# nano /etc/sysconfig/selinux
[root@ndbaranov ~]#
```

Изменение режима на Permissive

Редактируем конфигурационный файл для отключения SELinux (рис. [fig:002?], [fig:003?]).

The image consists of two terminal screenshots. The top screenshot shows the `/etc/sysconfig/selinux` file being edited in nano. The file content includes instructions on how to enable or disable SELinux, with the current state set to `SELINUX=disabled` and `SELINUXTYPE=targeted`. The bottom screenshot shows a sequence of commands: `su -` to switch to root, `getenforce` showing `Disabled`, `setenforce 1` showing `setenforce: SELinux is disabled`, and `nano /etc/sysconfig/selinux` to edit the file.

```
GNU nano 5.6.1 /etc/sysconfig/selinux Modified
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
# See also:
# https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/using_selinux/changing-selinux-state
#
# NOTE: Up to RHEL 8 release included, SELINUX=disabled would also
# fully disable SELinux during boot. If you need a system with SELinux
# fully disabled instead of SELinux running with no policy loaded, you
# need to pass selinux=0 to the kernel command line. You can use grubby
# to persistently set the bootloader to boot with selinux=0:
#
#   grubby --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
#   grubby --update-kernel ALL --remove-args selinux
#
SELINUX=disabled
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted

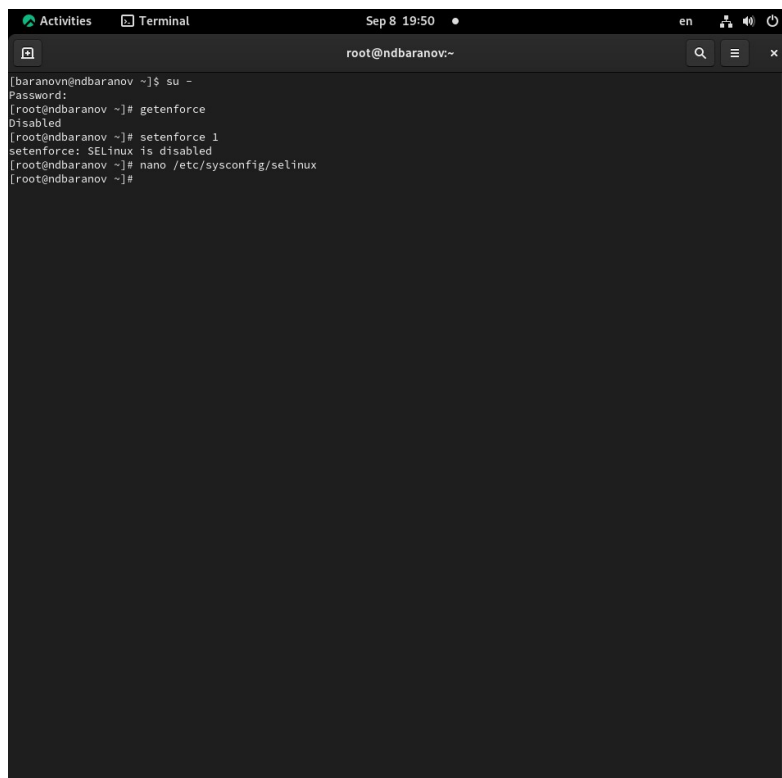
[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# getenforce
Disabled
[root@ndbaranov ~]# setenforce 1
setenforce: SELinux is disabled
[root@ndbaranov ~]# nano /etc/sysconfig/selinux
[root@ndbaranov ~]#
```

После перезагрузки проверяем статус SELinux (рис. [fig:003?]).

```
Activities Terminal Sep 8 19:50 en
root@ndbaranov:~
[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# getenforce
Disabled
[root@ndbaranov ~]# setenforce 1
setenforce: SELinux is disabled
[root@ndbaranov ~]# nano /etc/sysconfig/selinux
[root@ndbaranov ~]#
```

Проверка статуса после отключения

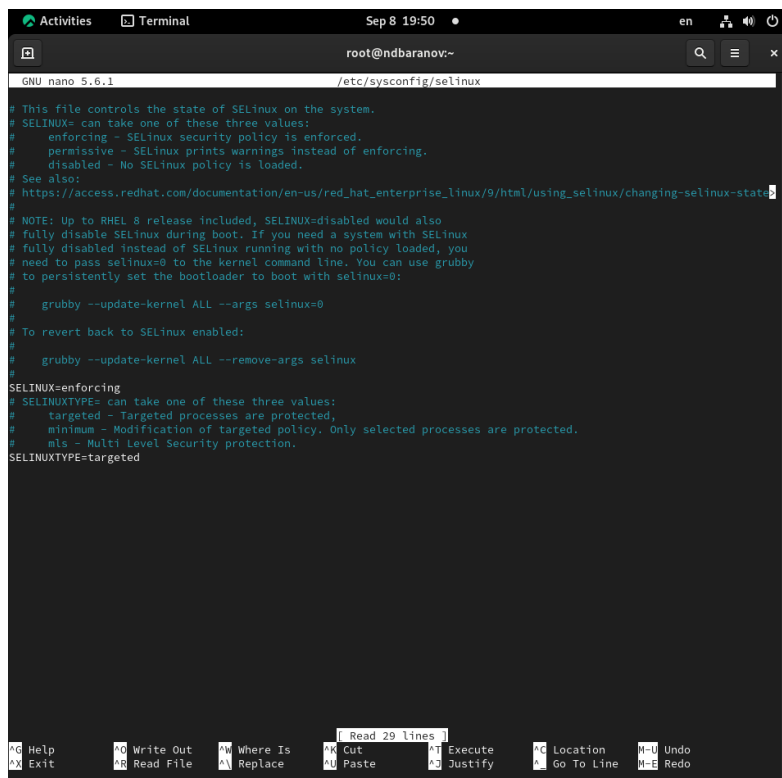
Пытаемся изменить режим работы SELinux при отключенном состоянии (рис. [fig:003?]).

A terminal window titled 'Terminal' with a date and time of 'Sep 8 19:50'. The prompt is 'root@ndbaranov:~'. The user has executed the following commands: 'su -', 'getenforce', 'setenforce 1', and 'nano /etc/sysconfig/selinux'. The output shows 'Disabled', 'setenforce: SELinux is disabled', and the nano editor prompt. The terminal window has a dark background and a light-colored text.

```
[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# getenforce
Disabled
[root@ndbaranov ~]# setenforce 1
setenforce: SELinux is disabled
[root@ndbaranov ~]# nano /etc/sysconfig/selinux
[root@ndbaranov ~]#
```

Попытка изменения режима при отключенном SELinux

Восстанавливаем режим enforcing через конфигурационный файл (рис. [fig:004?]).



```
GNU nano 5.6.1 /etc/sysconfig/selinux
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
# See also:
#   https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/using_selinux/changing-selinux-state
#
# NOTE: Up to RHEL 8 release included, SELINUX=disabled would also
#       fully disable SELinux during boot. If you need a system with SELinux
#       fully disabled instead of SELinux running with no policy loaded, you
#       need to pass selinux=0 to the kernel command line. You can use grubby
#       to persistently set the bootloader to boot with selinux=0:
#
#       grubby --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
#       grubby --update-kernel ALL --remove-args selinux
#
SELINUX=enforcing
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Восстановление режима enforcing

После перезагрузки проверяем статус SELinux (рис. [fig:005?]).


```
Activities Terminal Sep 8 19:53 en
root@ndbaranov:~
[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# sestatus -v
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:       /etc/selinux
Loaded policy name:            targeted
Current mode:                  enforcing
Mode from config file:         enforcing
Policy MLS status:             enabled
Policy deny_unknown status:    allowed
Memory protection checking:    actual (secure)
Max kernel policy version:    33

Process contexts:
Current context:               unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
Init context:                 system_u:system_r:init_t:s0
/usr/sbin/sshd                system_u:system_r:sshd_t:s0-s0:c0.c1023

File contexts:
Controlling terminal:         unconfined_u:object_r:user_devpts_t:s0
/etc/passwd                   system_u:object_r:passwd_file_t:s0
/etc/shadow                   system_u:object_r:shadow_t:s0
/bin/bash                     system_u:object_r:shell_exec_t:s0
/bin/login                    system_u:object_r:login_exec_t:s0
/bin/sh                       system_u:object_r:bin_t:s0 -> system_u:object_r:shell_exec_t:s0
/sbin/agetty                  system_u:object_r:getty_exec_t:s0
/sbin/init                    system_u:object_r:bin_t:s0 -> system_u:object_r:init_exec_t:s0
/usr/sbin/sshd                system_u:object_r:sshd_exec_t:s0
[root@ndbaranov ~]#
```

Проверка статуса после восстановления

3.2 Работа с контекстами безопасности

Просматриваем контекст безопасности файла /etc/hosts (рис. [fig:006?]).

```
Activities Terminal Sep 8 19:56 en root@ndbaranov:~
[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@ndbaranov ~]# cp /etc/hosts ~/
[root@ndbaranov ~]# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
[root@ndbaranov ~]# mv ~/hosts /etc
mv: overwrite '/etc/hosts'?
[root@ndbaranov ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@ndbaranov ~]# mv ~/hosts /etc
mv: overwrite '/etc/hosts'? y
[root@ndbaranov ~]# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
[root@ndbaranov ~]# restorecon -v /etc/hosts
Relabeled /etc/hosts from unconfined_u:object_r:admin_home_t:s0 to unconfined_u:object_r:net_conf_t:s0
[root@ndbaranov ~]# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
[root@ndbaranov ~]# touch /.autorelabel
[root@ndbaranov ~]#
```

Контекст безопасности /etc/hosts

Копируем файл и проверяем изменение контекста (рис. [fig:006?]).

```
Activities Terminal Sep 8 19:56 en
root@ndbaranov:~
[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@ndbaranov ~]# cp /etc/hosts ~/
[root@ndbaranov ~]# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
[root@ndbaranov ~]# mv ~/hosts /etc
mv: overwrite '/etc/hosts'?
[root@ndbaranov ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@ndbaranov ~]# mv ~/hosts /etc
mv: overwrite '/etc/hosts'? y
[root@ndbaranov ~]# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
[root@ndbaranov ~]# restorecon -v /etc/hosts
Relabeled /etc/hosts from unconfined_u:object_r:admin_home_t:s0 to unconfined_u:object_r:net_conf_t:s0
[root@ndbaranov ~]# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
[root@ndbaranov ~]# touch /.autorelabel
[root@ndbaranov ~]#
```

Копирование файла и проверка контекста

Перезаписываем файл и проверяем контекст (рис. [fig:006?]).

```
Activities Terminal Sep 8 19:56 en root@ndbaranov:~
[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@ndbaranov ~]# cp /etc/hosts ~/
[root@ndbaranov ~]# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
[root@ndbaranov ~]# mv ~/hosts /etc
mv: overwrite '/etc/hosts'?
[root@ndbaranov ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@ndbaranov ~]# mv ~/hosts /etc
mv: overwrite '/etc/hosts'? y
[root@ndbaranov ~]# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
[root@ndbaranov ~]# restorecon -v /etc/hosts
Relabeled /etc/hosts from unconfined_u:object_r:admin_home_t:s0 to unconfined_u:object_r:net_conf_t:s0
[root@ndbaranov ~]# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
[root@ndbaranov ~]# touch /.autorelabel
[root@ndbaranov ~]#
```

Перезапись файла и проверка контекста

Восстанавливаем правильный контекст безопасности (рис. [fig:006?]).

```
Activities Terminal Sep 8 19:56 en
root@ndbaranov:~
[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@ndbaranov ~]# cp /etc/hosts ~/
[root@ndbaranov ~]# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
[root@ndbaranov ~]# mv ~/hosts /etc
mv: overwrite '/etc/hosts'?
[root@ndbaranov ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@ndbaranov ~]# mv ~/hosts /etc
mv: overwrite '/etc/hosts'? y
[root@ndbaranov ~]# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
[root@ndbaranov ~]# restorecon -v /etc/hosts
Relabeled /etc/hosts from unconfined_u:object_r:admin_home_t:s0 to unconfined_u:object_r:net_conf_t:s0
[root@ndbaranov ~]# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
[root@ndbaranov ~]# touch /.autorelabel
[root@ndbaranov ~]#
```

Восстановление контекста restorecon

Создаем файл для массового восстановления контекстов (рис. [fig:006?]).

```
Activities Terminal Sep 8 19:56 en
root@ndbaranov:~
[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@ndbaranov ~]# cp /etc/hosts ~/
[root@ndbaranov ~]# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
[root@ndbaranov ~]# mv ~/hosts /etc
mv: overwrite '/etc/hosts'?
[root@ndbaranov ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@ndbaranov ~]# mv ~/hosts /etc
mv: overwrite '/etc/hosts'? y
[root@ndbaranov ~]# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
[root@ndbaranov ~]# restorecon -v /etc/hosts
Relabeled /etc/hosts from unconfined_u:object_r:admin_home_t:s0 to unconfined_u:object_r:net_conf_t:s0
[root@ndbaranov ~]# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
[root@ndbaranov ~]# touch /.autorelabel
[root@ndbaranov ~]#
```

Создание файла для массового восстановления

3.3 Настройка веб-сервера Apache с SELinux

Устанавливаем необходимое программное обеспечение (рис. [fig:007?]).

```
Activities Terminal Sep 8 20:00 en
root@ndbaranov/web

[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# dnf -y install httpd
*Last metadata expiration check: 2:09:20 ago on Mon 08 Sep 2025 05:49:52 PM MSK.
Package httpd-2.4.62-4.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@ndbaranov ~]# dnf -y install lynx
Last metadata expiration check: 2:09:34 ago on Mon 08 Sep 2025 05:49:52 PM MSK.
Dependencies resolved.
=====
Package Architecture Version Repository Size
=====
Installing:
lynx x86_64 2.8.9-20.el9 appstream 1.5 M
Transaction Summary
=====
Install 1 Package

Total download size: 1.5 M
Installed size: 6.1 M
Downloading Packages:
lynx-2.8.9-20.el9.x86_64.rpm 266 kB/s | 1.5 MB 00:05
-----
Total 137 kB/s | 1.5 MB 00:11
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing : 1/1
  Installing : lynx-2.8.9-20.el9.x86_64 1/1
  Running scriptlet: lynx-2.8.9-20.el9.x86_64 1/1
  Verifying : lynx-2.8.9-20.el9.x86_64 1/1

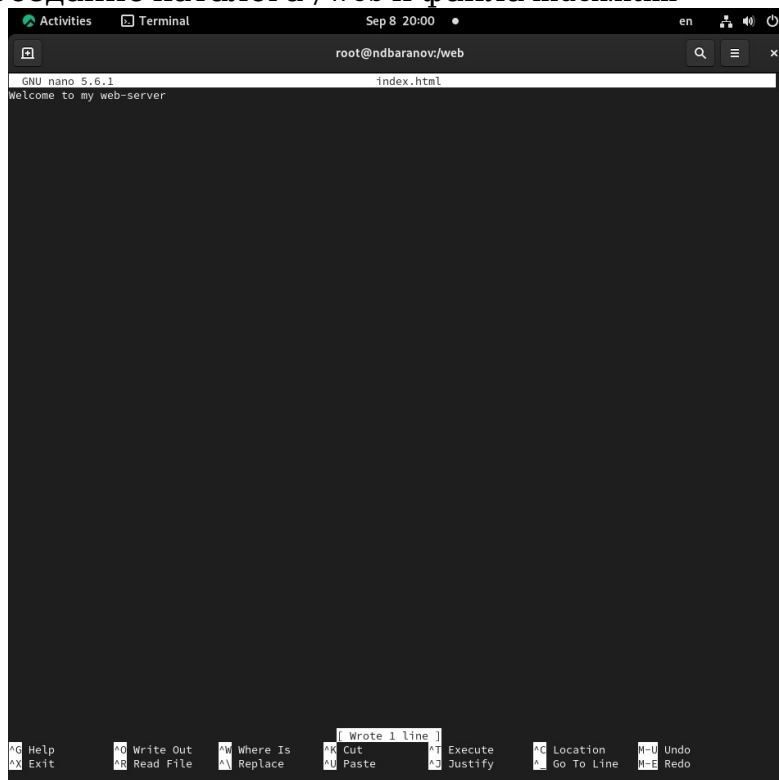
Installed:
lynx-2.8.9-20.el9.x86_64

Complete!
[root@ndbaranov ~]# mkdir /web
[root@ndbaranov ~]# cd /web
[root@ndbaranov web]# touch index.html
[root@ndbaranov web]#
```

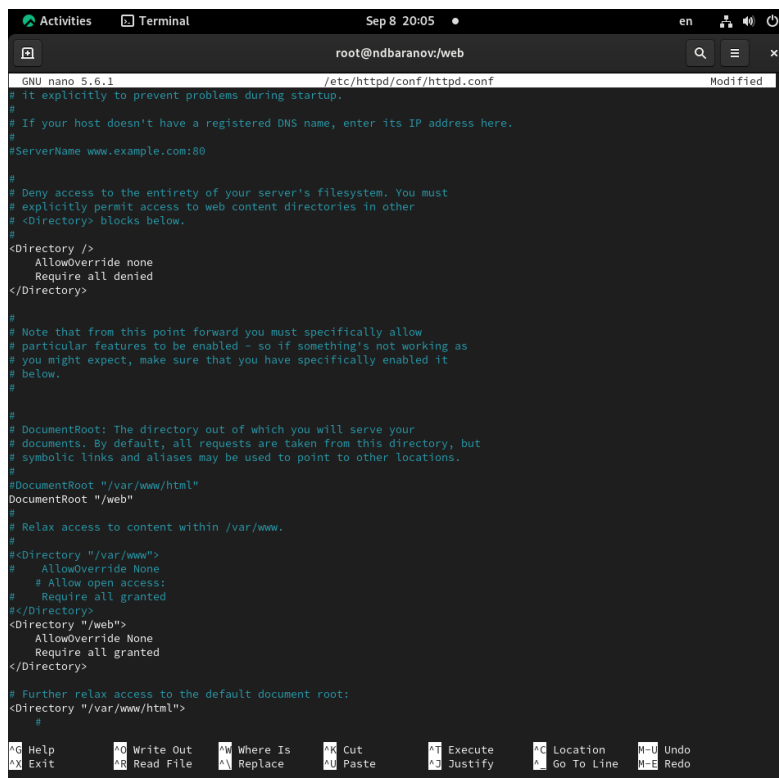
Установка httpd и lynx

Создаем каталог для веб-сервера и файл index.html (рис. [fig:007?], [fig:008?]).

Создание каталога /web и файла index.html



Настраиваем конфигурационный файл Apache (рис. [fig:009?]).



```
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf Modified
#
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
#ServerName www.example.com:80
#
# Deny access to the entirety of your server's filesystem. You must
# explicitly permit access to web content directories in other
# <Directory> blocks below.
#
<Directory />
    AllowOverride none
    Require all denied
</Directory>
#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
#DocumentRoot "/var/www/html"
DocumentRoot "/web"
#
# Relax access to content within /var/www.
#
<Directory "/var/www">
    # Allow override None
    # Allow open access:
    #   Require all granted
</Directory>
<Directory "/web">
    AllowOverride None
    Require all granted
</Directory>
#
# Further relax access to the default document root:
<Directory "/var/www/html">
    #
    # Help      Write Out  Where Is  Cut       Execute   Location  M-U  Undo
    # Exit      Read File  Replace  Paste     Justify   Go To Line M-B  Redo
```

Настройка httpd.conf

Запускаем и включаем веб-сервер (рис. [fig:010?]).

```
Activities Terminal Sep 8 20:05 en
root@ndbaranov/web

[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# dnf -y install httpd
*Last metadata expiration check: 2:09:20 ago on Mon 08 Sep 2025 05:49:52 PM MSK.
Package httpd-2.4.62-4.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@ndbaranov ~]# dnf -y install lynx
Last metadata expiration check: 2:09:34 ago on Mon 08 Sep 2025 05:49:52 PM MSK.
Dependencies resolved.
=====
Package Architecture Version Repository Size
=====
Installing:
lynx x86_64 2.8.9-20.el9 appstream 1.5 M
Transaction Summary
=====
Install 1 Package

Total download size: 1.5 M
Installed size: 6.1 M
Downloading Packages:
lynx-2.8.9-20.el9.x86_64.rpm 266 kB/s | 1.5 MB 00:05
-----
Total 137 kB/s | 1.5 MB 00:11
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing : 1/1
  Installing : lynx-2.8.9-20.el9.x86_64 1/1
  Running scriptlet: lynx-2.8.9-20.el9.x86_64 1/1
  Verifying : lynx-2.8.9-20.el9.x86_64 1/1
Installed:
lynx-2.8.9-20.el9.x86_64
Complete!
[root@ndbaranov ~]# mkdir /web
[root@ndbaranov ~]# cd /web
[root@ndbaranov web]# touch index.html
[root@ndbaranov web]# nano index.html
[root@ndbaranov web]# nano /etc/httpd/conf/httpd.conf
[root@ndbaranov web]# systemctl start httpd
[root@ndbaranov web]# systemctl enable httpd
[root@ndbaranov web]#
```

Запуск и включение httpd

Применяем правильный контекст безопасности для каталога /web (рис. [fig:012?]).

```
Activities Terminal Sep 8 20:06 en
root@ndbaranov/web

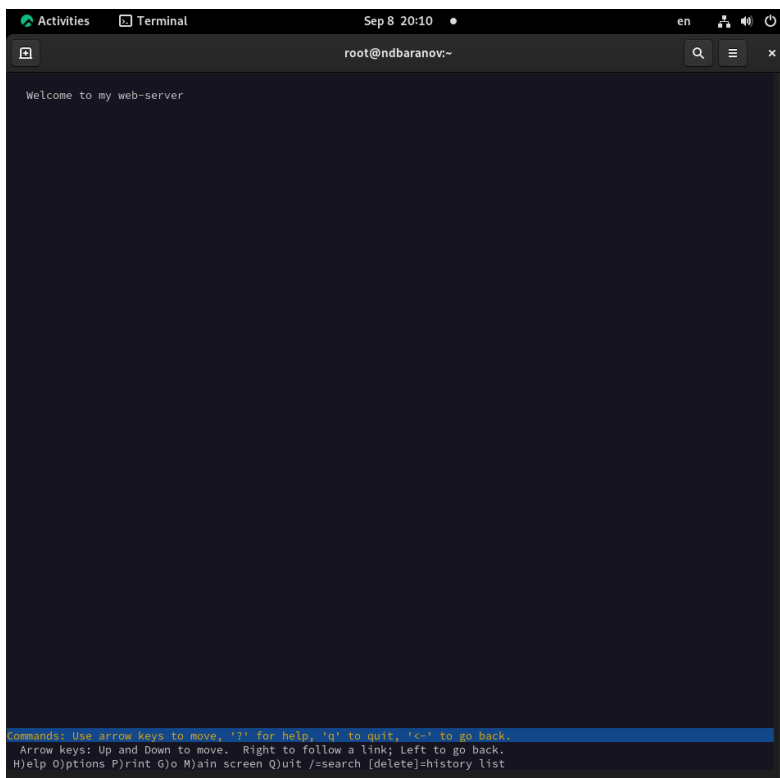
^[Last metadata expiration check: 2:09:20 ago on Mon 08 Sep 2025 05:49:52 PM MSK.
Package httpd-2.4.62-4.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@ndbaranov ~]# dnf -y install lynx
Last metadata expiration check: 2:09:34 ago on Mon 08 Sep 2025 05:49:52 PM MSK.
Dependencies resolved.
=====
Package Architecture Version Repository Size
=====
Installing:
lynx x86_64 2.8.9-20.el9 appstream 1.5 M
=====
Transaction Summary
=====
Install 1 Package

Total download size: 1.5 M
Installed size: 6.1 M
Downloading Packages:
lynx-2.8.9-20.el9.x86_64.rpm 266 kB/s | 1.5 MB 00:05
-----
Total 137 kB/s | 1.5 MB 00:11
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing : 1/1
Installing : lynx-2.8.9-20.el9.x86_64 1/1
Running scriptlet: lynx-2.8.9-20.el9.x86_64 1/1
Verifying : lynx-2.8.9-20.el9.x86_64 1/1
Installed:
lynx-2.8.9-20.el9.x86_64

Complete!
[root@ndbaranov ~]# mkdir /web
[root@ndbaranov ~]# cd /web
[root@ndbaranov web]# touch index.html
[root@ndbaranov web]# nano index.html
[root@ndbaranov web]# nano /etc/httpd/conf/httpd.conf
[root@ndbaranov web]# systemctl start httpd
[root@ndbaranov web]# systemctl enable httpd
[root@ndbaranov web]# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
[root@ndbaranov web]# restorecon -R -v /web
Relabeled /web from unconfined_u:object_r:default_t:s0 to unconfined_u:object_r:httpd_sys_content_t:s0
Relabeled /web/index.html from unconfined_u:object_r:default_t:s0 to unconfined_u:object_r:httpd_sys_content_t:s0
[root@ndbaranov web]#
```

Настройка контекста безопасности для /web

Проверяем доступ к веб-странице (рис. [fig:013?]).



Проверка доступа к веб-серверу

3.4 Управление переключателями SELinux для FTP

Просматриваем переключатели SELinux для службы FTP (рис. [fig:014?]).

```
Activities Terminal Sep 8 20:12 en
root@ndbaranov:~

[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# getsebool -a | grep ftp
ftpd_anon_write --> off
ftpd_connect_all_unreserved --> off
ftpd_connect_db --> off
ftpd_full_access --> off
ftpd_use_cifs --> off
ftpd_use_fusefs --> off
ftpd_use_nfs --> off
ftpd_use_passive_mode --> off
httpd_can_connect_ftp --> off
httpd_enable_ftp_server --> off
tftp_anon_write --> off
tftp_home_dir --> off
[root@ndbaranov ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (off , off) Allow ftpd to anon write
[root@ndbaranov ~]# setsebool ftpd_anon_write on
[root@ndbaranov ~]# getsebool ftpd_anon_write
ftpd_anon_write --> on
[root@ndbaranov ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (on , off) Allow ftpd to anon write
[root@ndbaranov ~]# setsebool -P ftpd_anon_write on
[root@ndbaranov ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (on , on) Allow ftpd to anon write
[root@ndbaranov ~]#
```

Просмотр переключателей FTP

Изменяем значение переключателя ftpd_anon_write (рис. [fig:014?]).

```
Activities Terminal Sep 8 20:12 en
root@ndbaranov:~

[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# getsebool -a | grep ftp
ftpd_anon_write --> off
ftpd_connect_all_unreserved --> off
ftpd_connect_db --> off
ftpd_full_access --> off
ftpd_use_cifs --> off
ftpd_use_fusefs --> off
ftpd_use_nfs --> off
ftpd_use_passive_mode --> off
httpd_can_connect_ftp --> off
httpd_enable_ftp_server --> off
tftp_anon_write --> off
tftp_home_dir --> off
[root@ndbaranov ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (off, off) Allow ftpd to anon write
[root@ndbaranov ~]# setsebool ftpd_anon_write on
[root@ndbaranov ~]# getsebool ftpd_anon_write
ftpd_anon_write --> on
[root@ndbaranov ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (on, off) Allow ftpd to anon write
[root@ndbaranov ~]# setsebool -P ftpd_anon_write on
[root@ndbaranov ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (on, on) Allow ftpd to anon write
[root@ndbaranov ~]#
```

Изменение переключателя ftpd_anon_write

Состояние переключателя ftpd_anon_write после изменения: - Время выполнения: включен (on) - Постоянная настройка: включена (on) - Описание: Allow ftpd to anon write (Разрешить анонимную запись для ftpd)

4. Выводы

Мы получили навыки работы с контекстом безопасности и политиками SELinux.

Список литературы