Создание и конфигурирование VM Centos 8 в VMware vSphere 7 для задания №1

```
sergey@ubuntu1:~/otus/selinux$ ansible-playbook newvm.yml

PLAY [start VM]
**********************************************************************************************************
TASK [deploy VM]
**********************************************************************************************************
changed: [localhost]
PLAY [VM configuration]
**********************************************************************************************************
TASK [enable selinux, disable firewalld, install and configure nginx]
**********************************************************************
changed: [selinux] => (item=sed -i 's/^SELINUX=.*/SELINUX=enforcing/g' /etc/selinux/config)
changed: [selinux] => (item=setenforce 1)
changed: [selinux] => (item=systemctl stop firewalld)
changed: [selinux] => (item=systemctl disable firewalld)
changed: [selinux] => (item=yum install -y nginx)
changed: [selinux] => (item=sed -i '/listen       80 default_server;/a listen       8092;' /etc/nginx/nginx.conf)

PLAY RECAP
**********************************************************************************************************
localhost                  : ok=1    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
selinux                    : ok=1    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```

Запуск nginx на нестандартном порту 3-мя разными способами

Проверим, что в ОС отключен файервол

```
[root@centos-se ~]# systemctl status firewalld

[root@centos-se ~]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
  Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor preset: enable>
  Active: inactive (dead)
    Docs: man:firewalld(1)
```

Проверим конфигурацию nginx:

```
[root@centos-se ~]# nginx -t

nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

Проверим режим работы SELinux:

```
[root@centos-se ~]# getenforce
Enforcing
```

Смотрим конфигурацию nginx:

```
[root@centos-se ~]# cat /etc/nginx/nginx.conf | grep listen

        listen       80 default_server;
listen       8092;
        listen       [::]:80 default_server;
#       listen       443 ssl http2 default_server;
```

listen [::]:443 ssl http2 default_server;
Пытаемся запустить nginx, не работает:

[root@centos-se nginx]# **systemctl start nginx.service**
Job for nginx.service failed because the control process exited with error code.
See "systemctl status nginx.service" and "journalctl -xe" for details.

Разрешим в SELinux работу nginx на порту TCP 8092 с помощью переключателей setsebool

Находим в логах (/var/log/audit/audit.log) информацию о блокировании порта

[root@centos-se ~]# **cat /var/log/audit/audit.log | grep 8092**
type=AVC msg=audit(1708009212.754:375): avc: denied { name_bind } for pid=4459 comm="nginx" src=8092 scontext=system_u:system_r:httpd_t:s0 tcontext=system_u:object_r:unreserved_port_t:s0 tclass=tcp_socket permissive=0

Копируем время, в которое был записан этот лог, и, с помощью утилиты audit2why смотрим информацию о запрете:

[root@centos-se ~]# **grep 1708009212.754:375 /var/log/audit/audit.log | audit2why**
type=AVC msg=audit(1708009212.754:375): avc: denied { name_bind } for pid=4459 comm="nginx" src=8092 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

Утилита audit2why покажет почему трафик блокируется.
Исходя из вывода утилиты, мы видим, что нам нужно поменять параметр nis_enabled.
Включим параметр nis_enabled и перезапустим nginx:

[root@centos-se ~]# **setsebool -P nis_enabled on**
[root@centos-se ~]# **systemctl restart nginx**
[root@centos-se ~]# **systemctl status nginx**
● nginx.service - The nginx HTTP and reverse proxy server
  Loaded: loaded (/usr/lib/systemd/system/nginx.service; disabled; vendor preset: disabled)
  Active: active (running) since Thu 2024-02-15 18:15:01 MSK; 10s ago
 Process: 4510 ExecStart=/usr/sbin/nginx (code=exited, status=0/SUCCESS)
 Process: 4508 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=0/SUCCESS)
 Process: 4507 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=0/SUCCESS)
Main PID: 4512 (nginx)
   Tasks: 2 (limit: 11126)
  Memory: 3.7M
  CGroup: /system.slice/nginx.service
          ├─4512 nginx: master process /usr/sbin/nginx
          └─4513 nginx: worker process

Feb 15 18:15:01 centos-se systemd[1]: Starting The nginx HTTP and reverse proxy server...
Feb 15 18:15:01 centos-se nginx[4508]: nginx: the configuration file /etc/nginx/nginx.conf sy>
Feb 15 18:15:01 centos-se nginx[4508]: nginx: configuration file /etc/nginx/nginx.conf test i>
Feb 15 18:15:01 centos-se systemd[1]: nginx.service: Failed to parse PID from file /run/nginx>
Feb 15 18:15:01 centos-se systemd[1]: Started The nginx HTTP and reverse proxy server.

Проверим статус параметра:

[root@centos-se ~]# **getsebool -a | grep nis_enabled**
nis_enabled --> on

Вернём запрет работы nginx на порту 8092 обратно.

[root@centos-se ~]# **setsebool -P nis_enabled off**

После отключения nis_enabled служба nginx снова не запустится.

разрешим в SELinux работу nginx на порту TCP 8092 с помощью добавления нестандартного порта в имеющийся тип:

Поиск имеющегося типа, для http трафика:

[root@centos-se ~]# **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

Добавим порт в тип http_port_t:

[root@centos-se ~]# **semanage port -a -t http_port_t -p tcp 8092**
[root@centos-se ~]# **semanage port -l | grep http_port_t**

```
http_port_t                tcp      8092, 80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t    tcp      5988
```

перезапустим службу nginx и проверим её работу:

```
[root@centos-se ~]# systemctl restart nginx
[root@centos-se ~]# systemctl status nginx

● nginx.service - The nginx HTTP and reverse proxy server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; disabled; vendor preset: disabled)
   Active: active (running) since Thu 2024-02-15 18:37:26 MSK; 15s ago
  Process: 4553 ExecStart=/usr/sbin/nginx (code=exited, status=0/SUCCESS)
  Process: 4550 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=0/SUCCESS)
  Process: 4549 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=0/SUCCESS)
 Main PID: 4555 (nginx)
    Tasks: 2 (limit: 11126)
   Memory: 3.7M
   CGroup: /system.slice/nginx.service
           ├─4555 nginx: master process /usr/sbin/nginx
           └─4556 nginx: worker process

Feb 15 18:37:26 centos-se systemd[1]: nginx.service: Failed with result 'timeout'.
Feb 15 18:37:26 centos-se systemd[1]: Stopped The nginx HTTP and reverse proxy server.
Feb 15 18:37:26 centos-se systemd[1]: Starting The nginx HTTP and reverse proxy server...
Feb 15 18:37:26 centos-se nginx[4550]: nginx: the configuration file /etc/nginx/nginx.conf sy>
Feb 15 18:37:26 centos-se nginx[4550]: nginx: configuration file /etc/nginx/nginx.conf test i>
Feb 15 18:37:26 centos-se systemd[1]: nginx.service: Failed to parse PID from file /run/nginx>
Feb 15 18:37:26 centos-se systemd[1]: Started The nginx HTTP and reverse proxy server.
```

Удалим нестандартный порт из имеющегося типа:

```
[root@centos-se ~]# semanage port -d -t http_port_t -p tcp 8092
[root@centos-se ~]# 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@centos-se ~]# systemctl restart nginx
Job for nginx.service failed because the control process exited with error code.
See "systemctl status nginx.service" and "journalctl -xe" for details.

[root@centos-se ~]# systemctl status nginx
● nginx.service - The nginx HTTP and reverse proxy server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; disabled; vendor preset: disabled)
   Active: failed (Result: exit-code) since Thu 2024-02-15 19:09:44 MSK; 11s ago
  Process: 4553 ExecStart=/usr/sbin/nginx (code=exited, status=0/SUCCESS)
  Process: 4587 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=1/FAILURE)
  Process: 4585 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=0/SUCCESS)
 Main PID: 4555 (code=exited, status=0/SUCCESS)

Feb 15 19:09:44 centos-se systemd[1]: nginx.service: Succeeded.
Feb 15 19:09:44 centos-se systemd[1]: Stopped The nginx HTTP and reverse proxy server.
Feb 15 19:09:44 centos-se systemd[1]: Starting The nginx HTTP and reverse proxy server...
Feb 15 19:09:44 centos-se nginx[4587]: nginx: the configuration file /etc/nginx/nginx.conf sy>
Feb 15 19:09:44 centos-se nginx[4587]: nginx: [emerg] bind() to 0.0.0.0:8092 failed (13: Perm>
…
Feb 15 19:09:44 centos-se systemd[1]: Failed to start The nginx HTTP and reverse proxy server.
```

Разрешим в SELinux работу nginx на порту TCP 8092 с помощью формирования и установки модуля SELinux

Пробуем снова запустить nginx:

[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 -xe" for details.

Смотрим логи SELinux, которые относятся к nginx:

[root@centos-se ~]# **grep nginx /var/log/audit/audit.log**
…
type=SYSCALL msg=audit(1708013785.517:405): arch=c000003e syscall=49 success=no exit=-13 a0=7 a1=5644973f6ce8 a2=10 a3=7fffbd7fe650 items=0 ppid=1 pid=4620 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(1708013785.519:406): 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"

Воспользуемся утилитой audit2allow для того, чтобы на основе логов SELinux сделать модуль, разрешающий работу nginx на нестандартном порту:

[root@ centos-se ~]# **grep nginx /var/log/audit/audit.log | audit2allow –M nginx**
****************** IMPORTANT ***********************
To make this policy package active, execute:

semodule -i nginx.pp

Audit2allow сформировал модуль, и сообщил нам команду, с помощью которой можно применить данный модуль

[root@centos-se ~]# **semodule -i nginx.pp**

Попробуем снова запустить nginx:

[root@centos-se ~]# **systemctl start nginx**
[root@centos-se ~]# **systemctl status nginx**
● nginx.service - The nginx HTTP and reverse proxy server
Loaded: loaded (/usr/lib/systemd/system/nginx.service; disabled; vendor preset: disabled)
Active: active (running) since Thu 2024-02-15 19:27:24 MSK; 8s ago
Process: 4660 ExecStart=/usr/sbin/nginx (code=exited, status=0/SUCCESS)
Process: 4658 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=0/SUCCESS)
Process: 4657 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=0/SUCCESS)
Main PID: 4662 (nginx)
Tasks: 2 (limit: 11126)
Memory: 3.7M
CGroup: /system.slice/nginx.service
├─4662 nginx: master process /usr/sbin/nginx
└─4663 nginx: worker process

Feb 15 19:27:24 centos-se systemd[1]: Starting The nginx HTTP and reverse proxy server...
Feb 15 19:27:24 centos-se *nginx*[4658]: nginx: the configuration file /etc/nginx/nginx.conf sy>
…
Feb 15 19:27:24 centos-se systemd[1]: Started The nginx HTTP and reverse proxy server.

После добавления модуля nginx запустился без ошибок. При использовании модуля изменения сохранятся после перезагрузки.
Просмотр всех установленных модулей: *semodule -l*
Для удаления модуля воспользуемся командой:

[root**@**centos-se **~]**# **semodule -r nginx**
libsemanage.semanage_direct_remove_key**:** Removing last nginx module **(**no
other nginx module exists at another priority**).**