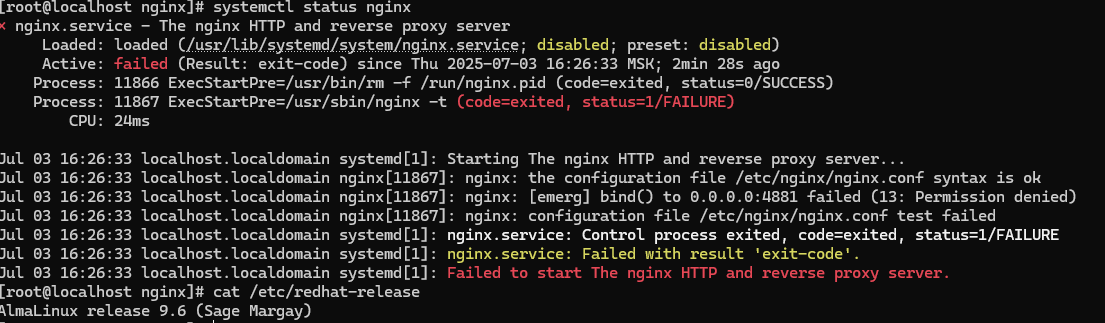
**Практика с SELinux**

1.Запустить nginx на нестандартном порту 3-мя разными способами:

Установлен alma linux 9.6. Устновлен nginx, настроен на порт 4881

При запуске получаю ошибку



Проверяю фаервол

systemctl status firewalld

Он включен, останавливаю его

systemctl stop firewalld

systemctl disable firewalld

Проверяю конфигурацию nginx

[root@localhost nginx]# nginx -t

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

nginx: configuration file /etc/nginx/nginx.conf test is successful

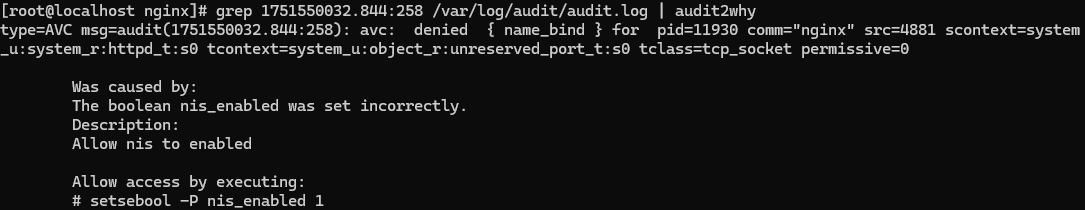
Проверяю Selinux

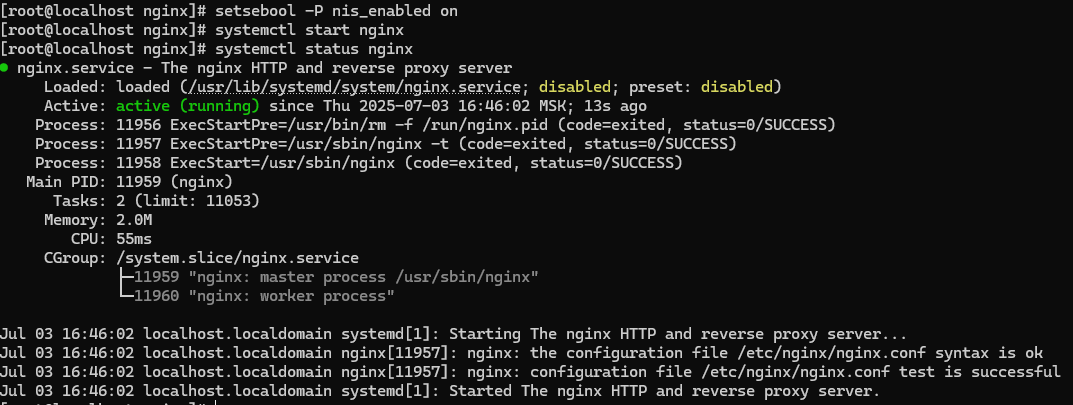
[root@localhost nginx]# getenforce

Enforcing

- setsebool

В /var/log/audit/audit.log на хожу ниформацию о блокировании. Смотрю запись в логи при помощи утилиты audit2why

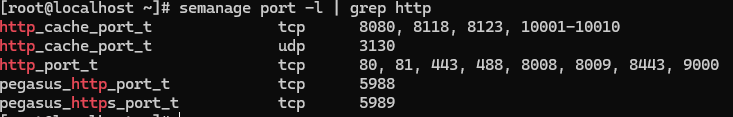
  
  
Включим параметр nis\_enabled и перезапустим nginx: setsebool -P nis\_enabled on



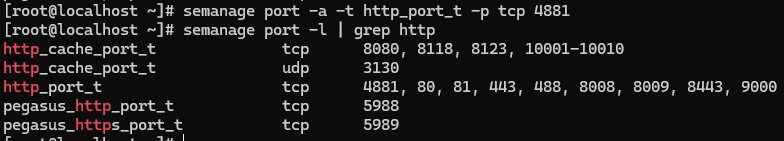
Отключаю обратно setsebool -P nis\_enabled off

- добавление нестандартного порта в имеющийся тип

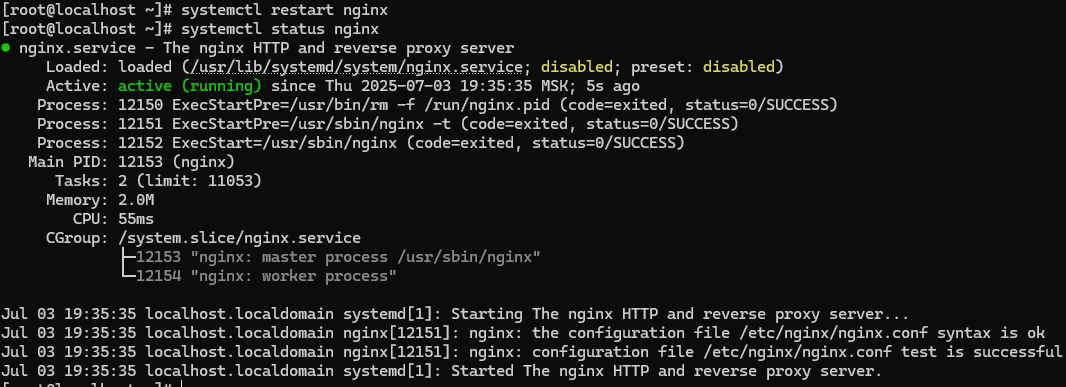
Поиск имеющегося типа, для http трафика



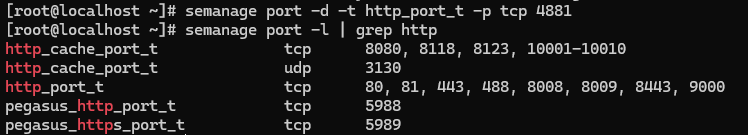
Добавим порт в тип http\_port\_t



Перезапускаем nginx и проверяем статус

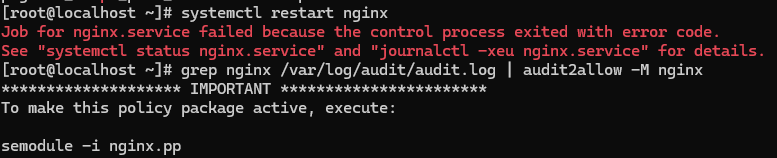


Удалить нестандартный порт из имеющегося типа http\_port\_t

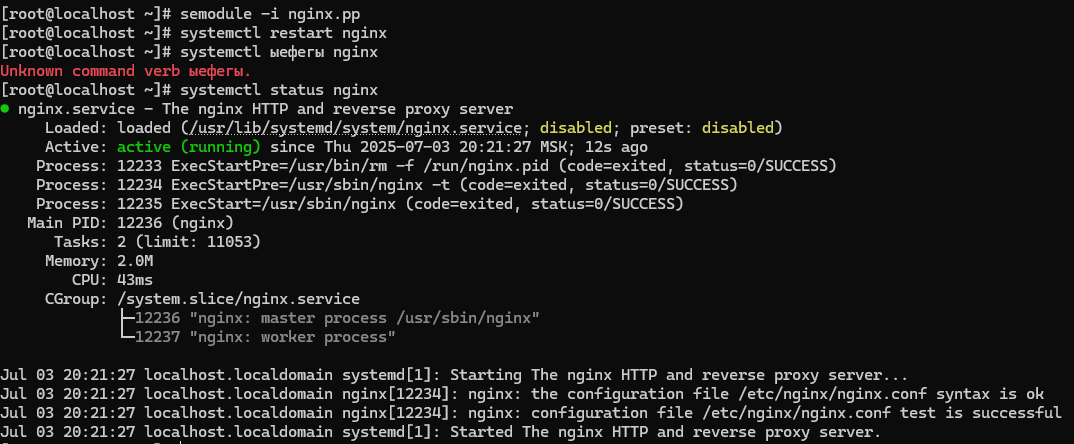


- формирование и установка модуля SELinux

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



Применяем сформированный модуль



Смотрим установленные модули



Удаляем модуль



2. Обеспечить работоспособность приложения при включенном selinux

Для выполнения лабораторной установил git, ansible, vagrant, virtualbox

Выполнил клонирование репозитария:

*git clone https://github.com/mbfx/otus-linux-adm.git*

В директории otus-linux-adm/selinux\_dns\_problems разварачиваю 2 ВМ с помощью vagrant:

*vagrant up*

При первом запуске появились ошибки ansible при установке пакетов. На обеих ВМ в yum заменил пути для репозитариев:

*sed -i s/mirror.centos.org/vault.centos.org/g /etc/yum.repos.d/\*.repo*

*sed -i s/^#.\*baseurl=http/baseurl=http/g /etc/yum.repos.d/\*.repo*

*sed -i s/^mirrorlist=http/#mirrorlist=http/g /etc/yum.repos.d/\*.repo*

*sed -i 's/mirrorlist/#mirrorlist/g' /etc/yum.repos.d/CentOS-\**

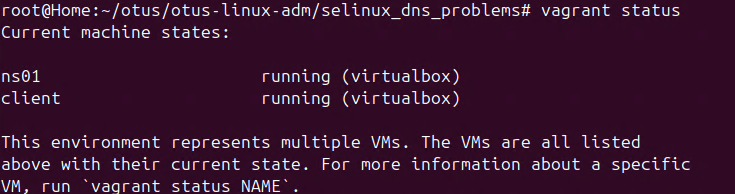
*sed -i 's|#baseurl=http://mirror.centos.org|baseurl=http://vault.centos.org|g' /etc/yum.repos.d/CentOS-\**

*yum clean all*

Повторно запустил provision: *vagrant provision*

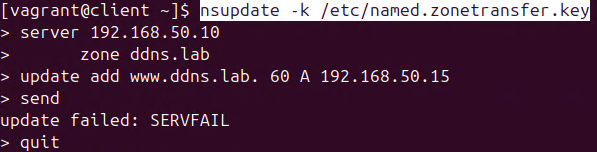
Выполнилось без ошибок. Стенд развернут.

*vagrant status*

**

Подключаюсь к client: *vagrant ssh client*

Пробую внести изменения в зону: *nsupdate -k /etc/named.zonetransfer.key*

**

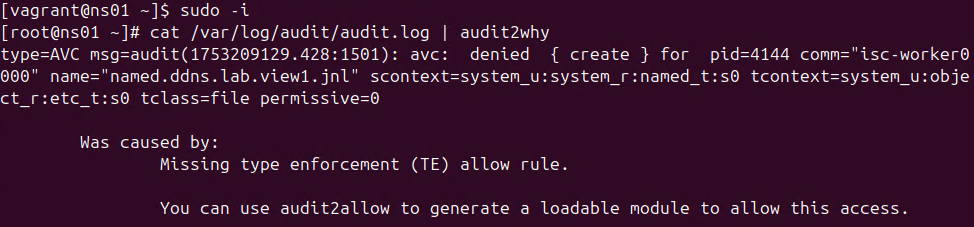
Изменения внести не удалось. Смотрим логи SELinux



Ошибки отсутствуют.

Подключаемся к ns01: *vagrant ssh ns01*

Смотрим ошибки SELinux:

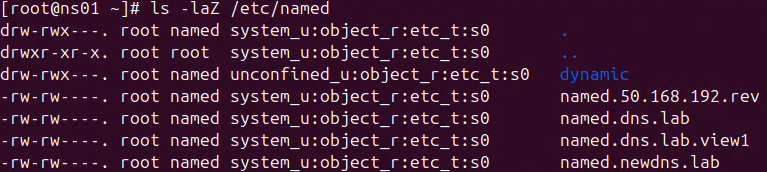


В логах мы видим, что ошибка в контексте безопасности. Целевой контекст **etc\_t**.

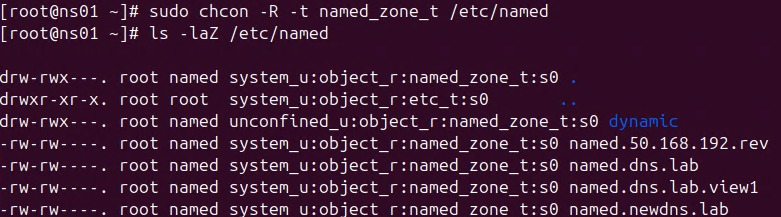
Для сравнения посмотрим существующую зону (localhost) и её контекст



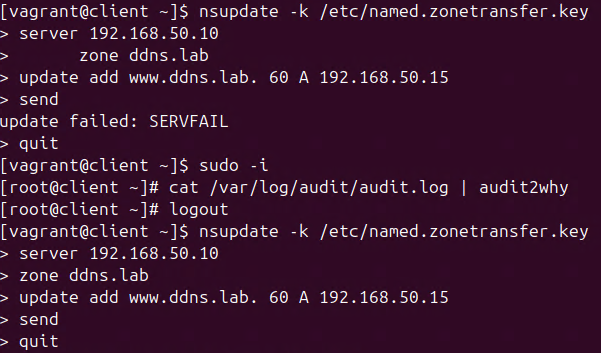
Проверяем контекст на файлах /etc/named:



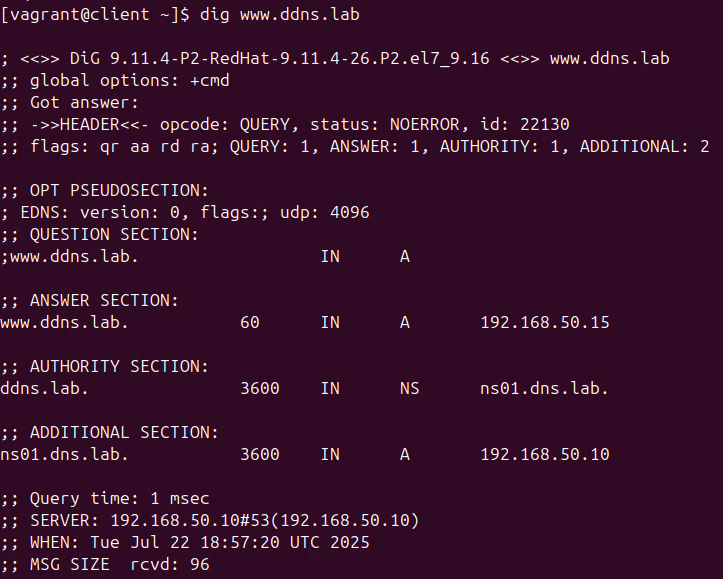
Видим, что контекст безопасности неправильный. Меняем контекст безопасности на правильный для каталога /etc/named: *sudo chcon -R -t named\_zone\_t /etc/named*



Снова проверяем возможность внесения изменений на клиенте:



При помощи dig смотрим информацию о зоне:



Видим, что изменения применились