Обеспечение работоспособности приложения при включенном SELinux

$ git clone https://github.com/mbfx/otus-linux-adm.git
Cloning into 'otus-linux-adm'...
remote: Enumerating objects: 558, done.
remote: Counting objects: 100% (456/456), done.
remote: Compressing objects: 100% (303/303), done.
remote: Total 558 (delta 125), reused 396 (delta 74), pack-reused 102
Receiving objects: 100% (558/558), 1.38 MiB | 4.12 MiB/s, done.
Resolving deltas: 100% (140/140), done.

$ cd otus-linux-adm/selinux_dns_problems
$ vagrant up
$ vagrant status
Current machine states:
ns01 running (virtualbox)
client running (virtualbox)
This environment represents multiple VMs. The VMs are all listed
above with their current state. For more information about a specific
VM, run `vagrant status NAME`.

$ vagrant ssh client
Last login: Fri Feb 16 08:44:06 2024 from 10.0.2.2
################################
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!
################################

[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

Изменения внести не получилось. Смотрим логи SELinux

[vagrant@client ~]$ sudo -i
[root@client ~]# cat /var/log/audit/audit.log | audit2why
[root@client ~]#
На клиенте отсутствуют ошибки.
Не закрывая сессию на клиенте, подключимся к серверу ns01 и проверим логи SELinux:

$ vagrant ssh ns01
Last login: Fri Feb 16 08:41:17 2024 from 10.0.2.2

[vagrant@ns01 ~]$ sudo -i
[root@ns01 ~]# cat /var/log/audit/audit.log | audit2why
type=AVC msg=audit(1708072878.487:1916): avc: denied { write } for pid=5243 comm="isc-worker0000" name="named" dev="sda1" ino=67548216 scontext=system_u:system_r:named_t:s0 tcontext=system_u:object_r:named_zone_t:s0 tclass=dir permissive=0

Was caused by:
The boolean named_write_master_zones was set incorrectly.
Description:
Allow named to write master zones

Allow access by executing:
# setsebool -P named_write_master_zones 1
type=AVC msg=audit(1708073338.777:1941): avc: denied { create } for pid=5243 comm="isc-worker0000" name="named.ddns.lab.view1.jnl" scontext=system_u:system_r:named_t:s0 tcontext=system_u:object_r:etc_t:s0 tclass=file permissive=0

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

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

1)Логическое значение name_write_master_zones установлено неправильно.

[root@ns01 ~]# setsebool -P named_write_master_zones 1

*2) Ошибка в контексте безопасности. Вместо типа **named_t** используется тип **etc_t**.*
Проверим проблему 2) в каталоге /etc/named

[root@ns01 ~]# ls -laZ /etc/named
drw-rwx---. root named system_u:object_r:etc_t:s0 .
drwxr-xr-x. root root system_u:object_r:etc_t:s0 ..
drw-rwx---. root named unconfined_u:object_r:etc_t:s0 dynamic
-rw-rw----. root named system_u:object_r:etc_t:s0 named.50.168.192.rev
-rw-rw----. root named system_u:object_r:etc_t:s0 named.dns.lab
-rw-rw----. root named system_u:object_r:etc_t:s0 named.dns.lab.view1
-rw-rw----. root named system_u:object_r:etc_t:s0 named.newdns.lab

Контекст безопасности неправильный. Проблема в том, что конфигурационные файлы лежат в другом каталоге.
Смотрим в каком каталоги должны лежать, файлы, чтобы на них распространялись правильные политики SELinux

[root@ns01 ~]# sudo semanage fcontext -l | grep named

```
/etc/rndc.*                     regular file    system_u:object_r:named_conf_t:s0
/var/named(/.*)?                  all files     system_u:object_r:named_zone_t:s0
…
```

Изменим тип контекста безопасности для каталога /etc/named

[root@ns01 ~]# sudo chcon -R -t named_zone_t /etc/named
[root@ns01 ~]# ls -laZ /etc/named
```
drw-rwx---. root named system_u:object_r:named_zone_t:s0 .
drwxr-xr-x. root root  system_u:object_r:etc_t:s0      ..
drw-rwx---. root named unconfined_u:object_r:named_zone_t:s0 dynamic
-rw-rw----. root named system_u:object_r:named_zone_t:s0 named.50.168.192.rev
-rw-rw----. root named system_u:object_r:named_zone_t:s0 named.dns.lab
-rw-rw----. root named system_u:object_r:named_zone_t:s0 named.dns.lab.view1
-rw-rw----. root named system_u:object_r:named_zone_t:s0 named.newdns.lab
```

вносим изменения с клиента:

[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
> quit
```

[vagrant@client ~]$ dig www.ddns.lab

```
; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.15 <<>> www.ddns.lab
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26798
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.ddns.lab.                  IN      A

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

;; AUTHORITY SECTION:
ddns.lab.               3600    IN      NS      ns01.dns.lab.

;; ADDITIONAL SECTION:
ns01.dns.lab.           3600    IN      A       192.168.50.10

;; Query time: 7 msec
;; SERVER: 192.168.50.10#53(192.168.50.10)
;; WHEN: Fri Feb 16 10:19:34 UTC 2024
;; MSG SIZE  rcvd: 96
```

Изменения применились.
Перезагружаем хосты и ещё раз делаем запрос с помощью dig:

[vagrant@client ~]$ dig @192.168.50.10 www.ddns.lab

```
; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.15 <<>> @192.168.50.10 www.ddns.lab
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18008
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.ddns.lab.                IN      A

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

;; AUTHORITY SECTION:
ddns.lab.              3600    IN      NS      ns01.dns.lab.

;; ADDITIONAL SECTION:
ns01.dns.lab.          3600    IN      A       192.168.50.10

;; Query time: 1 msec
;; SERVER: 192.168.50.10#53(192.168.50.10)
;; WHEN: Fri Feb 16 10:27:13 UTC 2024
;; MSG SIZE  rcvd: 96
```

Настройки сохранились