```
################################
### Enjoy! ####################
################################
[vagrant@client ~]$ sudo -i
[root@client ~]# nsupdate -k /etc/named.zonetransfer.key
> server 192.168.56.10
> zone ddns.lab
> update add www.ddns.lab 60 192.168.56.15
'192.168.56.15' is not a valid class or type: unknown class/type
> send
> ^[[A^[[A^[[B
> correct section name:
> update add www.ddns.lab 60 A 192.168.56.15
> send
update failed: SERVFAIL
> quit


[root@client ~]# cat /var/log/audit/audit.log | audit2why
[root@client ~]#


[vagrant@ns01 ~]$ sudo -i
[root@ns01 ~]# cat /var/log/audit/audit.log | audit2why
type=AVC msg=audit(1646671477.566:1985): avc:  denied  { create } for  pid=5278 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.

[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.56.168.192.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
```

```
[root@ns01 ~]# semanage permissive -a named_t


[root@client ~]# nsupdate -k /etc/named.zonetransfer.key
> server 192.168.56.10
> zone ddns.lab
> update add test1.ddns.lab 60 A 192.168.56.15
> send
> quit
[root@client ~]# dig test1.ddns.lab
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;test1.ddns.lab.                IN      A
;; AUTHORITY SECTION:
.               679     IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2022030700 1800 900 604800
86400
;; Query time: 26 msec
```

[root@ns01 ~]# grep "AVC" /var/log/audit/audit.log
type=AVC msg=audit(1646673324.216:71): avc: denied { write } for pid=645 comm="isc-worker0000" name="named.ddns.lab.view1.jnl" dev="sda1" ino=465007 scontext=system_u:system_r:named_t:s0 tcontext=system_u:object_r:etc_t:s0 tclass=file permissive=0

[root@ns01 ~]# tail -f /var/log/messages | grep SELinux
Mar 7 17:20:04 ns01 setroubleshoot: SELinux is preventing isc-worker0000 from write access on the file named.ddns.lab.view1.jnl. For complete SELinux messages run: sealert -l 6c4a18bb-9df5-4323-99b3-a2f8e87873f1

Mar 7 17:20:04 ns01 python: SELinux is preventing isc-worker0000 from write access on the file named.ddns.lab.view1.jnl.#012#012***** Plugin catchall_labels (83.8 confidence) suggests **********#012#012If you want to allow isc-worker0000 to have write access on the named.ddns.lab.view1.jnl file#012Then you need to change the label on named.ddns.lab.view1.jnl#012Do#012# semanage fcontext -a -t FILE_TYPE 'named.ddns.lab.view1.jnl'#012where FILE_TYPE is one of the following: afs_cache_t, dnssec_trigger_var_run_t, initrc_tmp_t, ipa_var_lib_t, krb5_host_rcache_t, krb5_keytab_t, named_cache_t, named_log_t, named_tmp_t, named_var_run_t, named_zone_t, puppet_tmp_t, user_cron_spool_t, user_tmp_t.#012Then execute:#012restorecon -v 'named.ddns.lab.view1.jnl'#012#012#012***** Plugin catchall (17.1 confidence) suggests **********#012#012If you believe that isc-worker0000 should be allowed write access on the named.ddns.lab.view1.jnl file by default.#012Then you should report this as a bug.#012You can generate a local policy module to allow this access.#012Do#012allow this access for now by executing:#012# ausearch -c 'isc-worker0000' --raw | audit2allow -M my-iscworker0000#012# semodule -i my-iscworker0000.pp#012

```
[root@ns01 ~]# sealert -a /var/log/audit/audit.log
Additional Information:
Source Context              system_u:system_r:named_t:s0
Target Context              system_u:object_r:etc_t:s0
Target Objects              named.ddns.lab.view1.jnl [ file ]
Source                      isc-worker0000
Source Path                 /usr/sbin/named
Port                        <Unknown>
Host                        <Unknown>
Source RPM Packages         bind-9.11.4-26.P2.el7_9.9.x86_64
Target RPM Packages
Policy RPM                  selinux-policy-3.13.1-266.el7.noarch
Selinux Enabled             True
Policy Type                 targeted
Enforcing Mode              Enforcing
Host Name                   ns01
Platform                    Linux ns01 3.10.0-1127.el7.x86_64 #1 SMP Tue Mar
                            31 23:36:51 UTC 2020 x86_64 x86_64
Alert Count                 3
First Seen                  2022-03-07 17:11:11 UTC
Last Seen                   2022-03-07 17:15:24 UTC
Local ID                    619a2aa6-2a5a-4065-acbd-5ba465fdf597

Raw Audit Messages
type=AVC msg=audit(1646673324.216:71): avc:  denied  { write } for  pid=645 comm="isc-worker0000"
name="named.ddns.lab.view1.jnl" dev="sda1" ino=465007 scontext=system_u:system_r:named_t:s0
tcontext=syst
em_u:object_r:etc_t:s0 tclass=file permissive=0


type=SYSCALL msg=audit(1646673324.216:71): arch=x86_64 syscall=open success=no exit=EACCES
a0=7efc023cf018 a1=2 a2=1b6 a3=24 items=0 ppid=1 pid=645 auid=4294967295 uid=25 gid=25 euid=25
suid=25 fsuid=25
egid=25 sgid=25 fsgid=25 tty=(none) ses=4294967295 comm=isc-worker0000 exe=/usr/sbin/named
subj=system_u:system_r:named_t:s0 key=(null)

Hash: isc-worker0000,named_t,etc_t,file,write
```