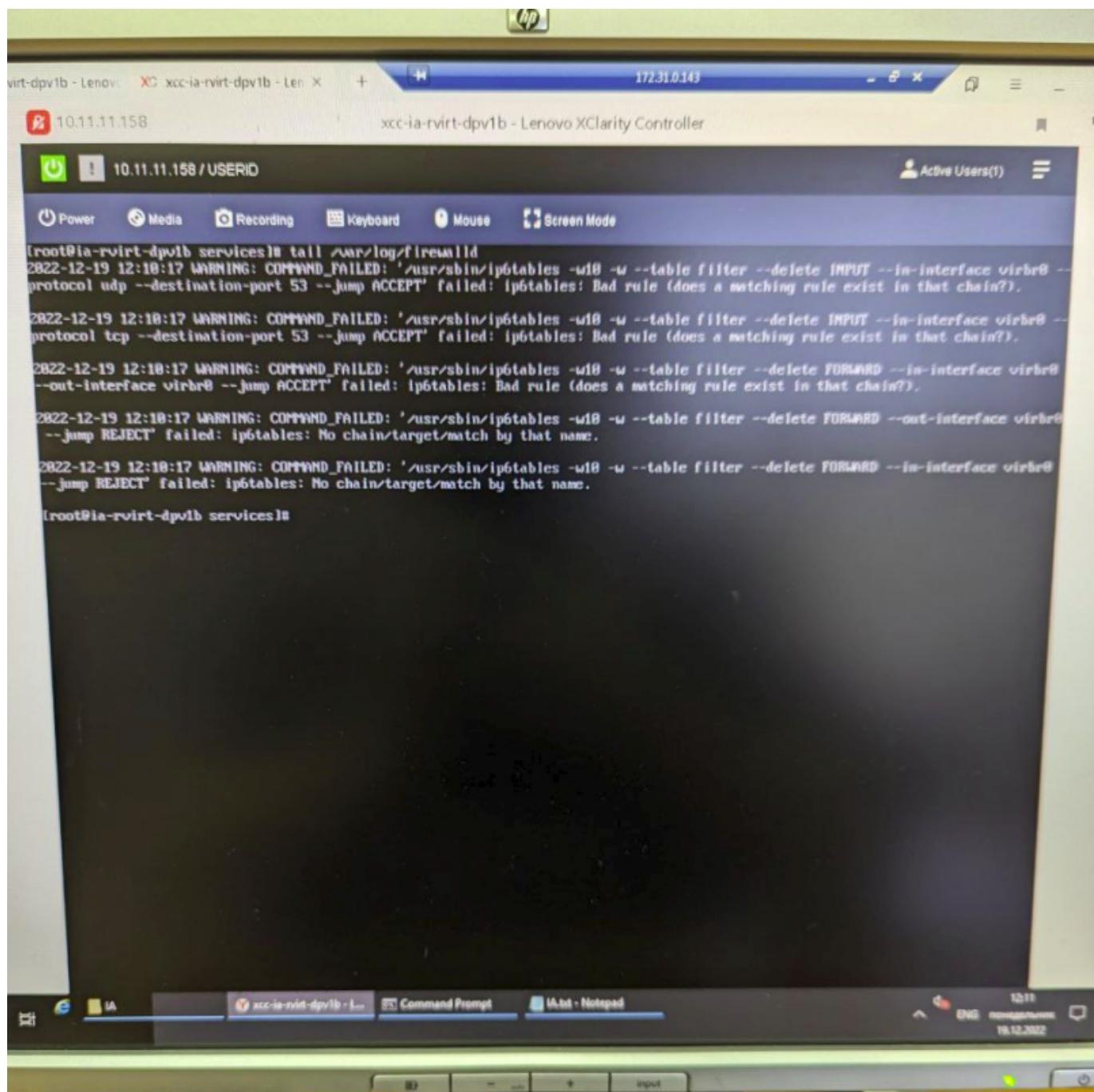


Конфигурация csd_firewalld не успевает применяться после перезапуска сервера и он уходит в постоянную перезагрузку

Симптомы

После перезапуска сервера виртуализации на нем долго запускается сеть и в конечном счете сервер перезапускается. Журнал /var/log/firewalld содержит записи о поврежденных файлах конфигурации.



The screenshot shows a terminal window with the title 'virt-dpv1b - Lenovo XC xcc-ia-rvirt-dpv1b - Len' and the IP address '172.31.0.143'. The window displays a log of errors from the 'firewalld' service. The errors are related to failed iptables commands, specifically attempting to delete rules that do not exist in the 'virbr8' chain. The log entries are as follows:

```
[root@ia-rvirt-dpv1b services]# tail /var/log/firewalld
2022-12-19 12:18:17 WARNING: COMMAND_FAILED: '/usr/sbin/iptables -w18 -w --table filter --delete INPUT --in-interface virbr8 --protocol udp --destination-port 53 --jump ACCEPT' failed: ip6tables: Bad rule (does a matching rule exist in that chain?).

2022-12-19 12:18:17 WARNING: COMMAND_FAILED: '/usr/sbin/iptables -w18 -w --table filter --delete INPUT --in-interface virbr8 --protocol tcp --destination-port 53 --jump ACCEPT' failed: ip6tables: Bad rule (does a matching rule exist in that chain?).

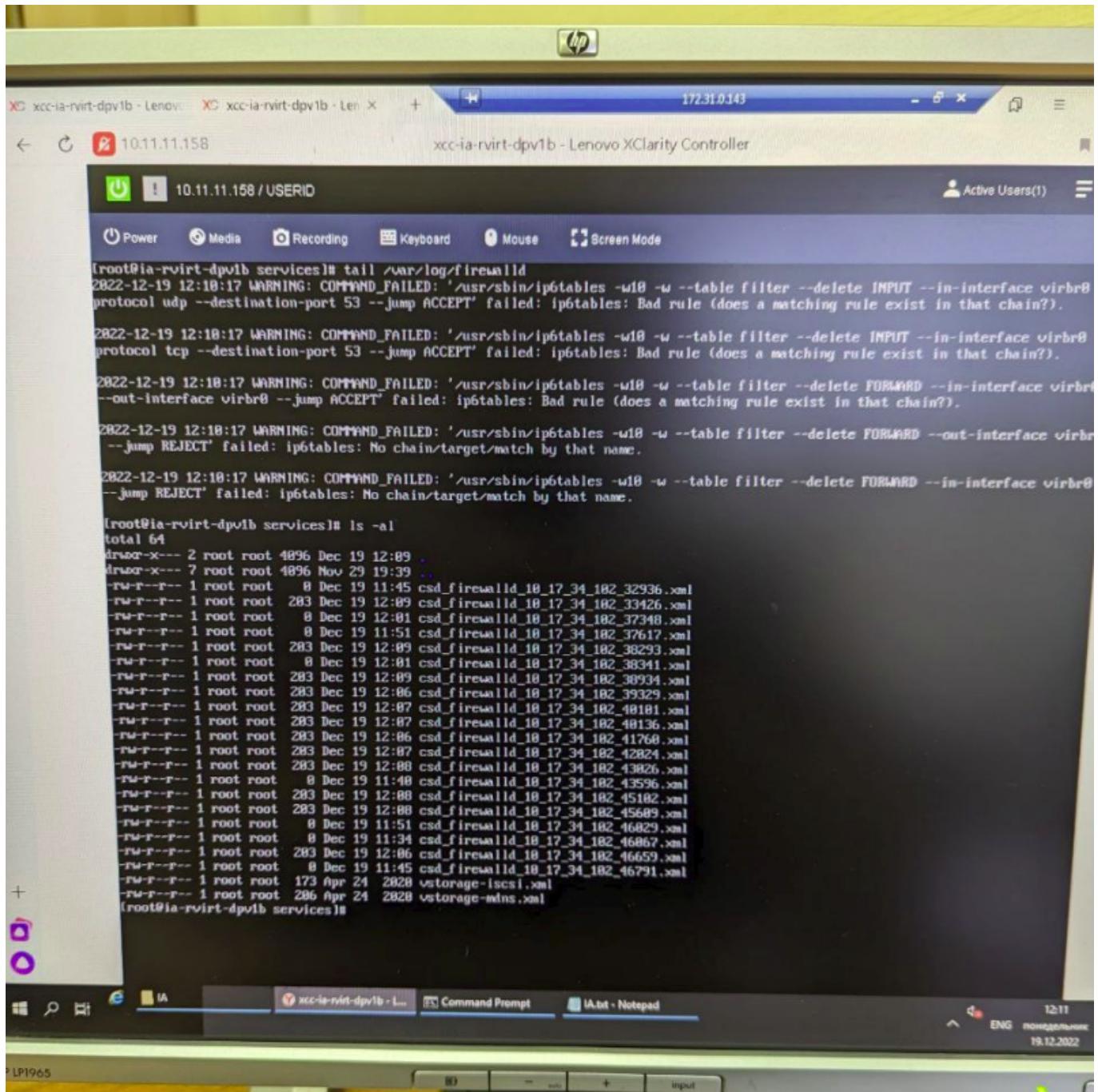
2022-12-19 12:18:17 WARNING: COMMAND_FAILED: '/usr/sbin/iptables -w18 -w --table filter --delete FORWARD --in-interface virbr8 --out-interface virbr8 --jump ACCEPT' failed: ip6tables: Bad rule (does a matching rule exist in that chain?).

2022-12-19 12:18:17 WARNING: COMMAND_FAILED: '/usr/sbin/iptables -w18 -w --table filter --delete FORWARD --out-interface virbr8 --jump REJECT' failed: ip6tables: No chain/target/match by that name.

2022-12-19 12:18:17 WARNING: COMMAND_FAILED: '/usr/sbin/iptables -w18 -w --table filter --delete FORWARD --in-interface virbr8 --jump REJECT' failed: ip6tables: No chain/target/match by that name.

[root@ia-rvirt-dpv1b services]#
```

Некоторые файлы в директории /etc/firewalld/services/ имеют нулевой размер.



Причины

- При запуске каждого CS создается отдельное правило брандмауэра. В некоторых случаях, при перезапуске сервера правила не успевают создаться до окончания времени, отведенного серверу на занрузку и менеджер кластера shaman перезагружает указанный сервер.

Восстановление

1. Выключить проблемный узел;

2. Исключить проблемный узел из конфигурации кластера командой: `shaman leave -n <IP_хранилища_цикличной_ноды>;`
3. Включить проблемный узел;
4. Добавить сетевой интерфейс кластерного взаимодействия в доверенную сеть, командой:
`firewall-cmd --permanent --zone=trusted --add-interface=<ifname_of_storage_if> && firewall-cmd --reload;`
5. Отключить сервис `csd_firewalld`, командой: `systemctl stop csd_firewalld && systemctl disable csd_firewalld;`
6. Удалить все конфигурационные файлы `csd` в директории `/etc/firewalld/services/`, командой `rm -rf /etc/firewalld/services/csd_*.xml;`

From:

<https://micronode.ru/> - **micronode.ru**



Permanent link:

https://micronode.ru/wiki/trouble/rosplatforma/firewalld_cyclic_reboot

Last update: **2022/12/19 19:09**