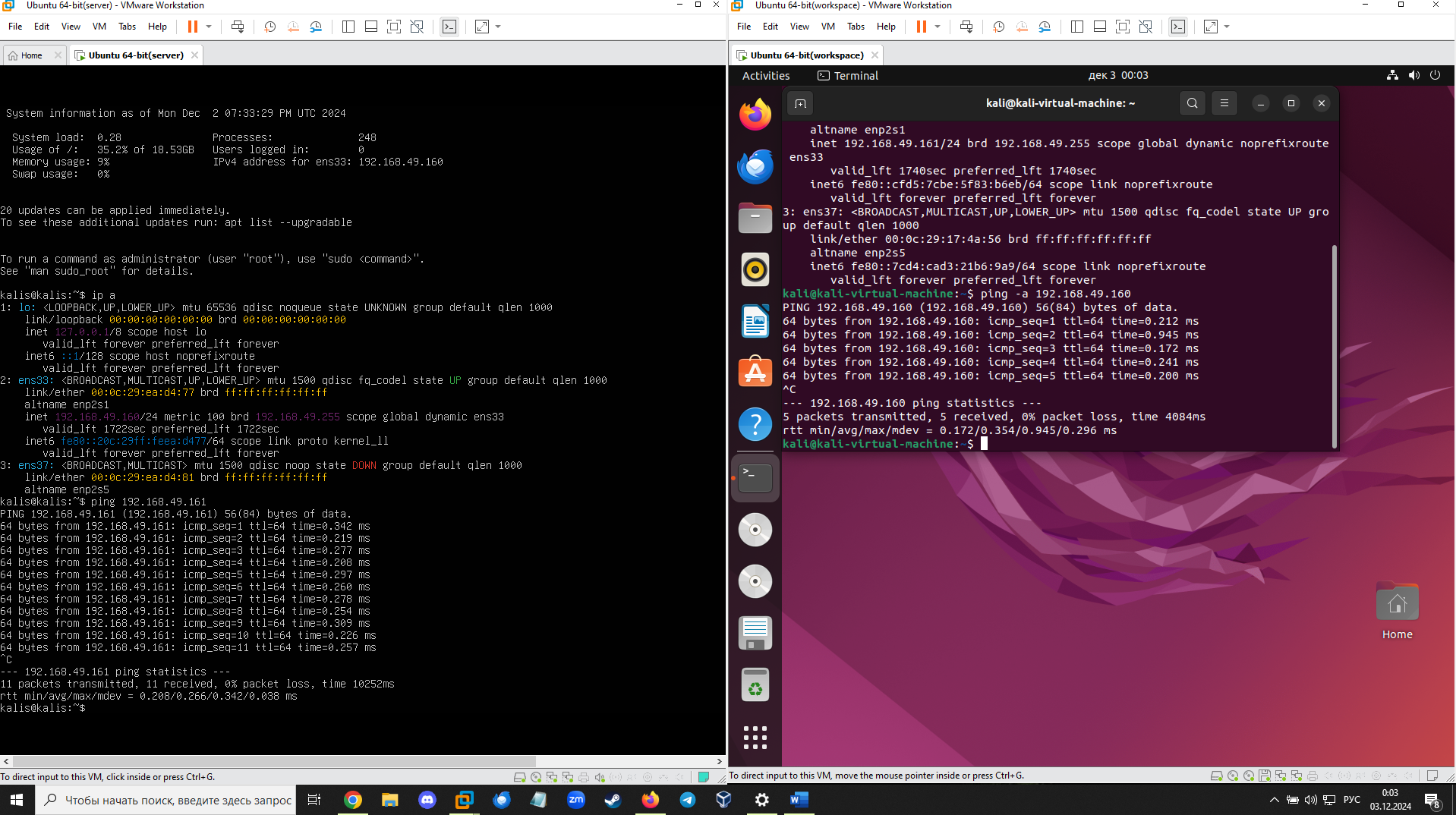
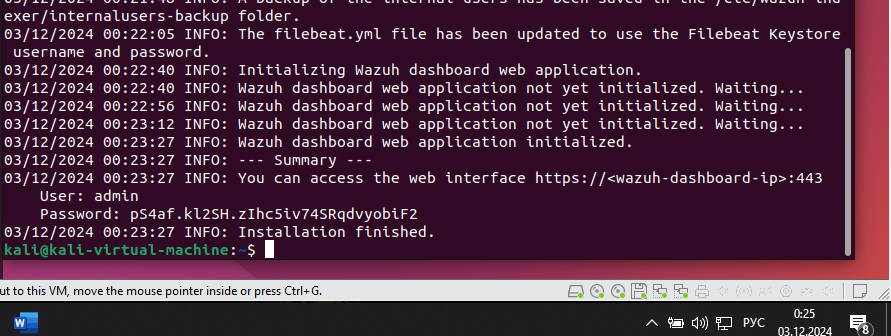
ПРЗ 5 Threat Hunting

1. Разверните виртуальные машины (минимум 2 – сервер и агенты)
2. Обеспечить между ними сетевой обмен.



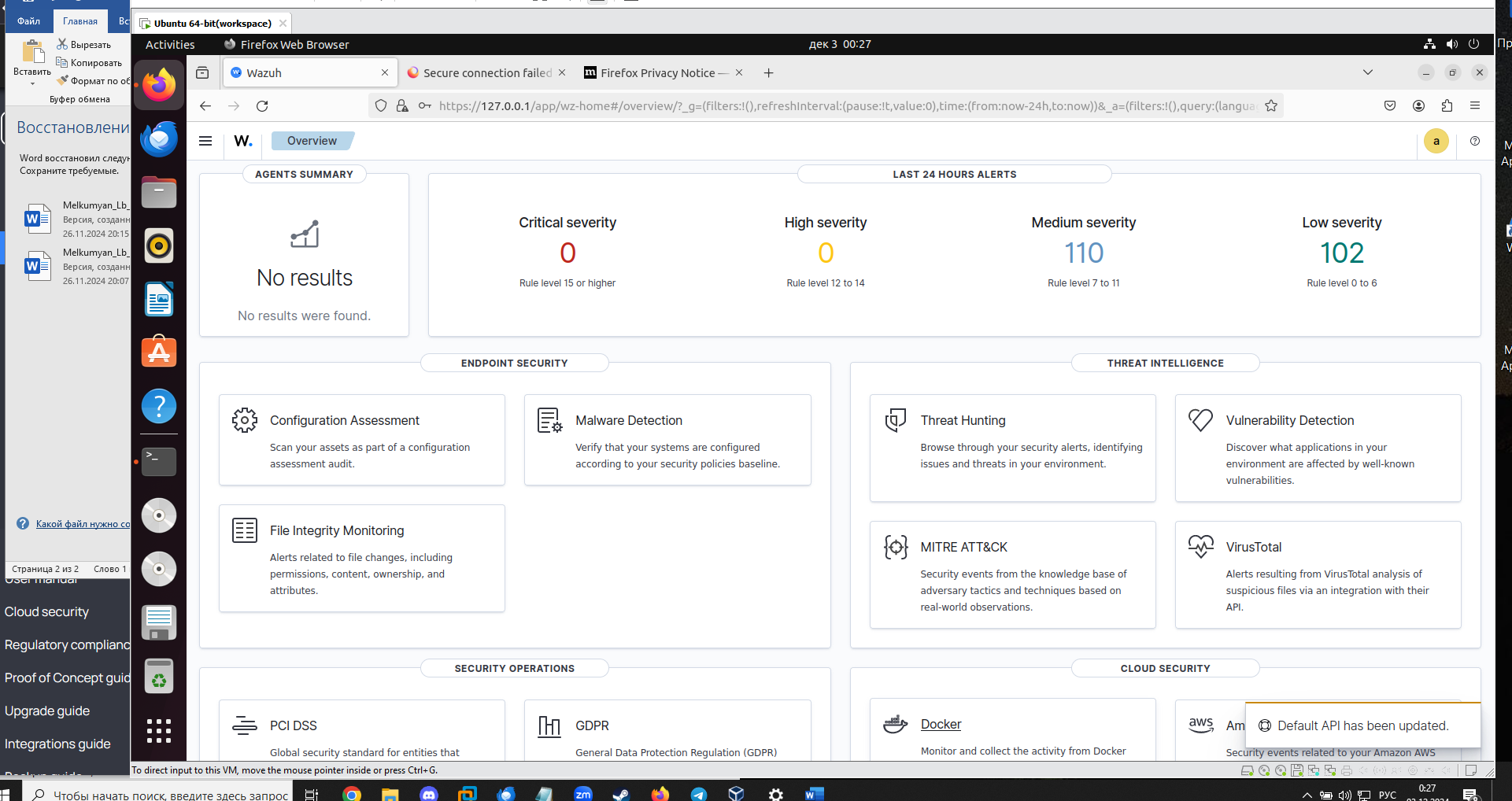
1. Развернуть на одной из ВМ сервер Wazuh



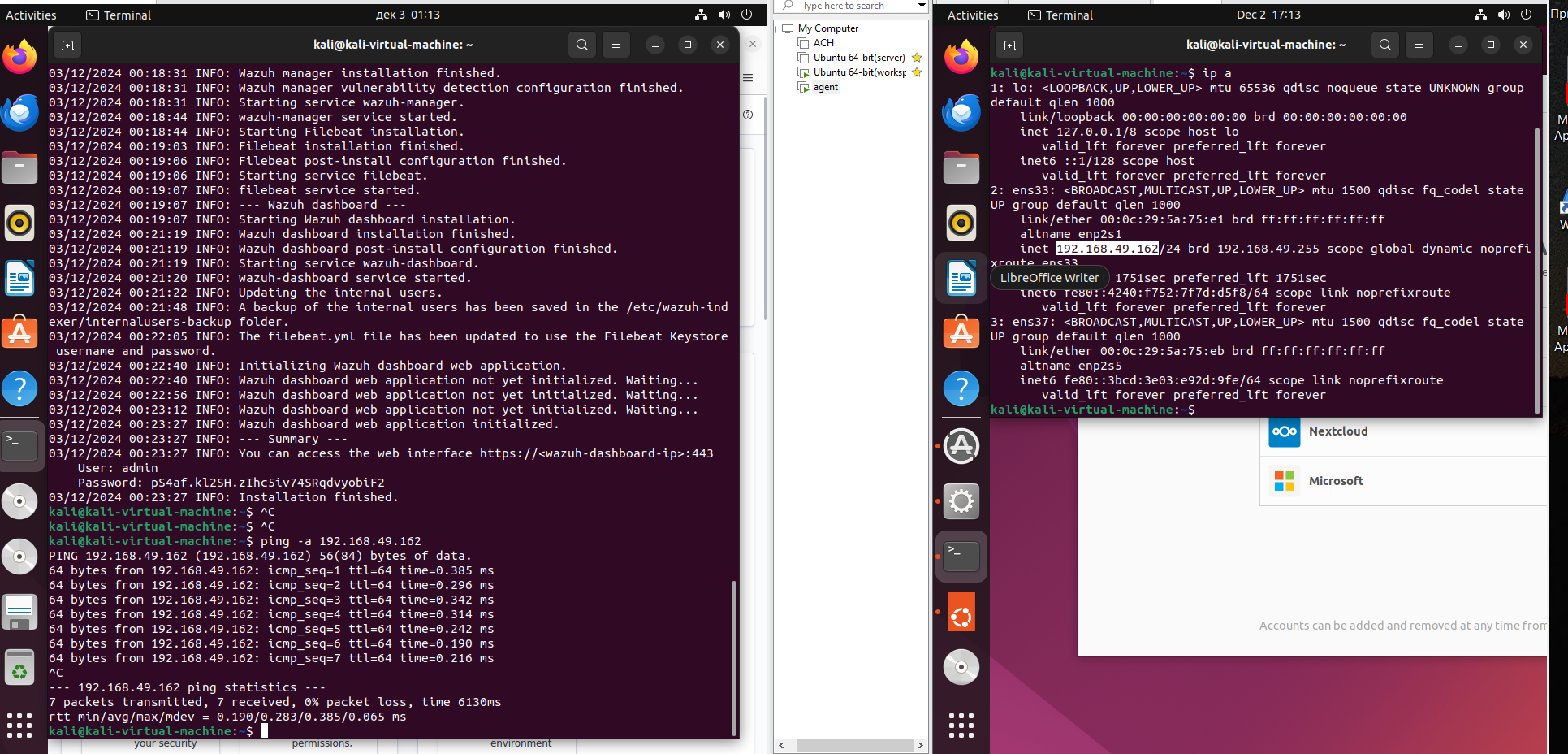
User: admin

Password: pS4af.kl2SH.zIhc5iv74SRqdvyobiF2

Зашли на сам Wazuh

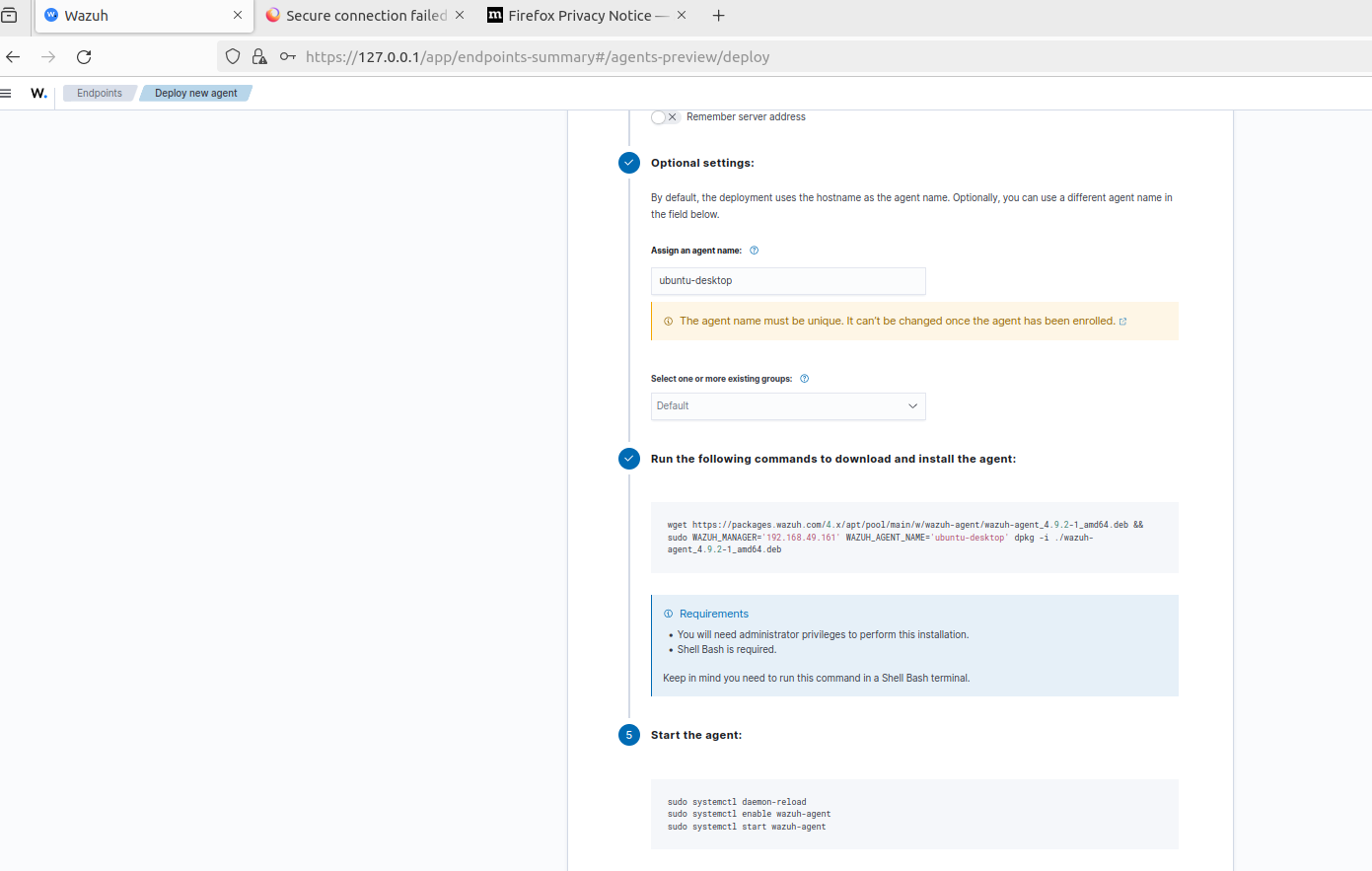


Еще раз проверил сетевую связанность между машинами потому что будучи сонным установил не туда,и пришлось еще одну машину разворачивать

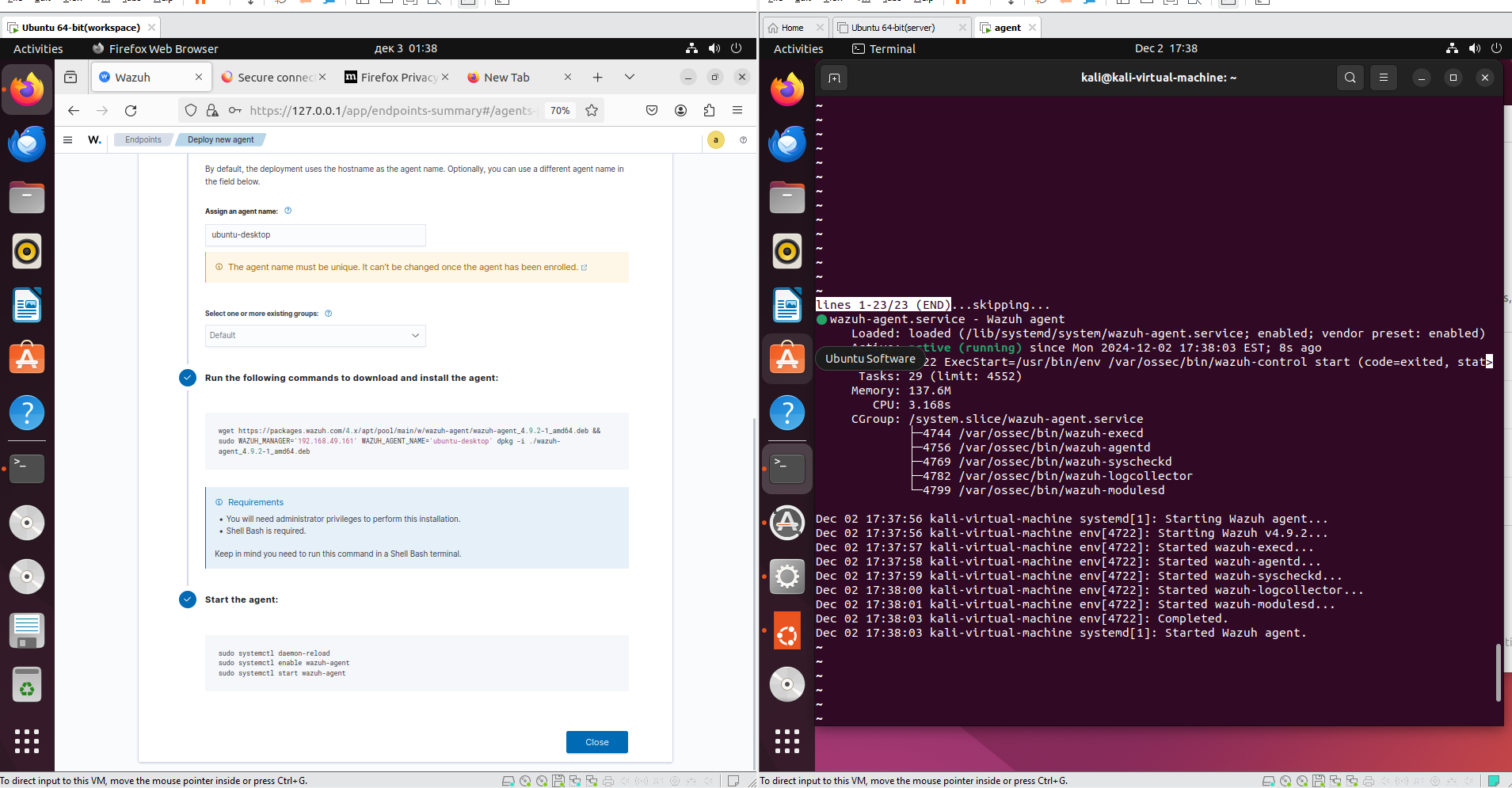


1. Подключите агента используя документацию

Устанавливаю агента через Wazuh



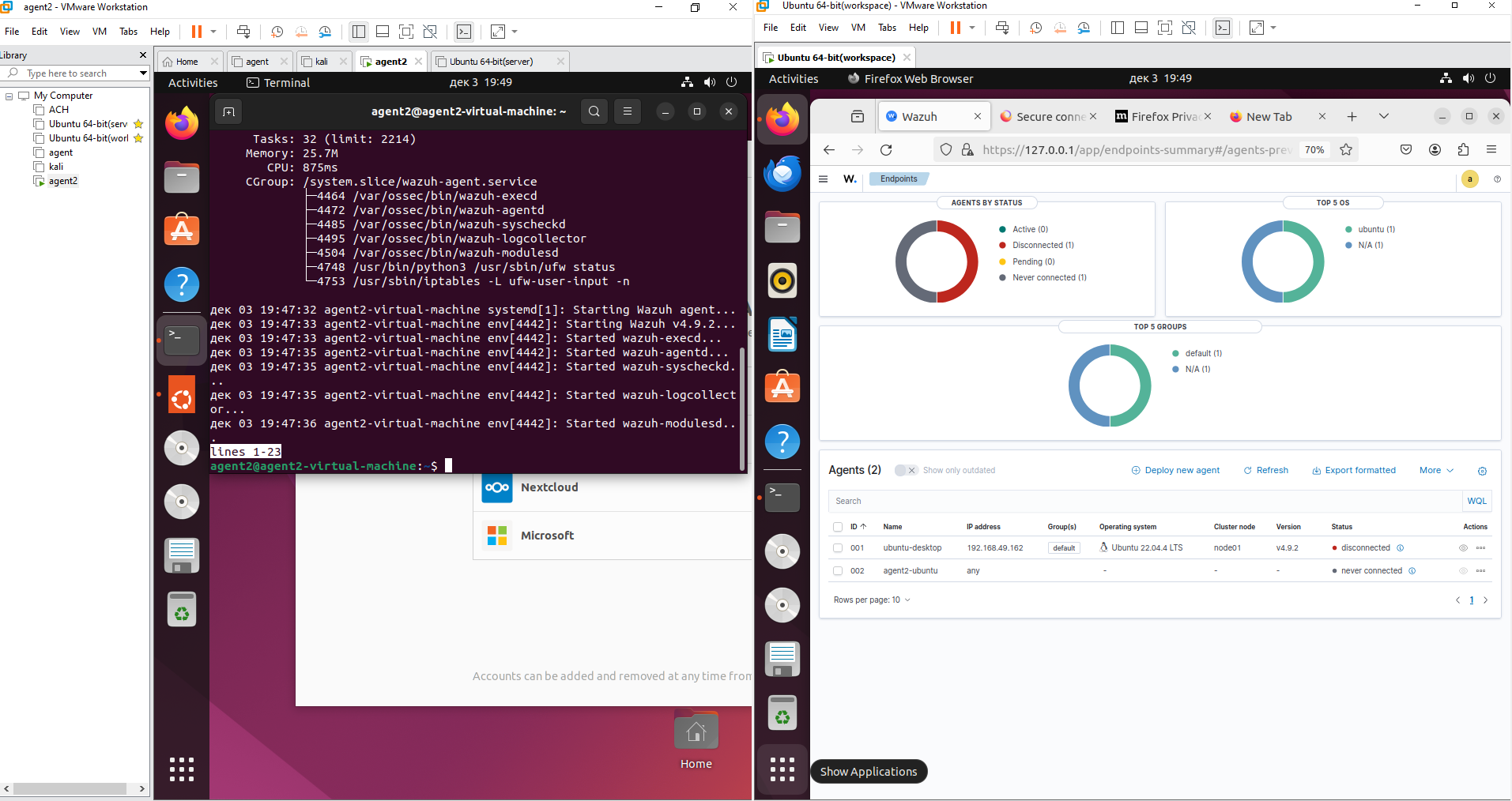
Ввели все команды и установили



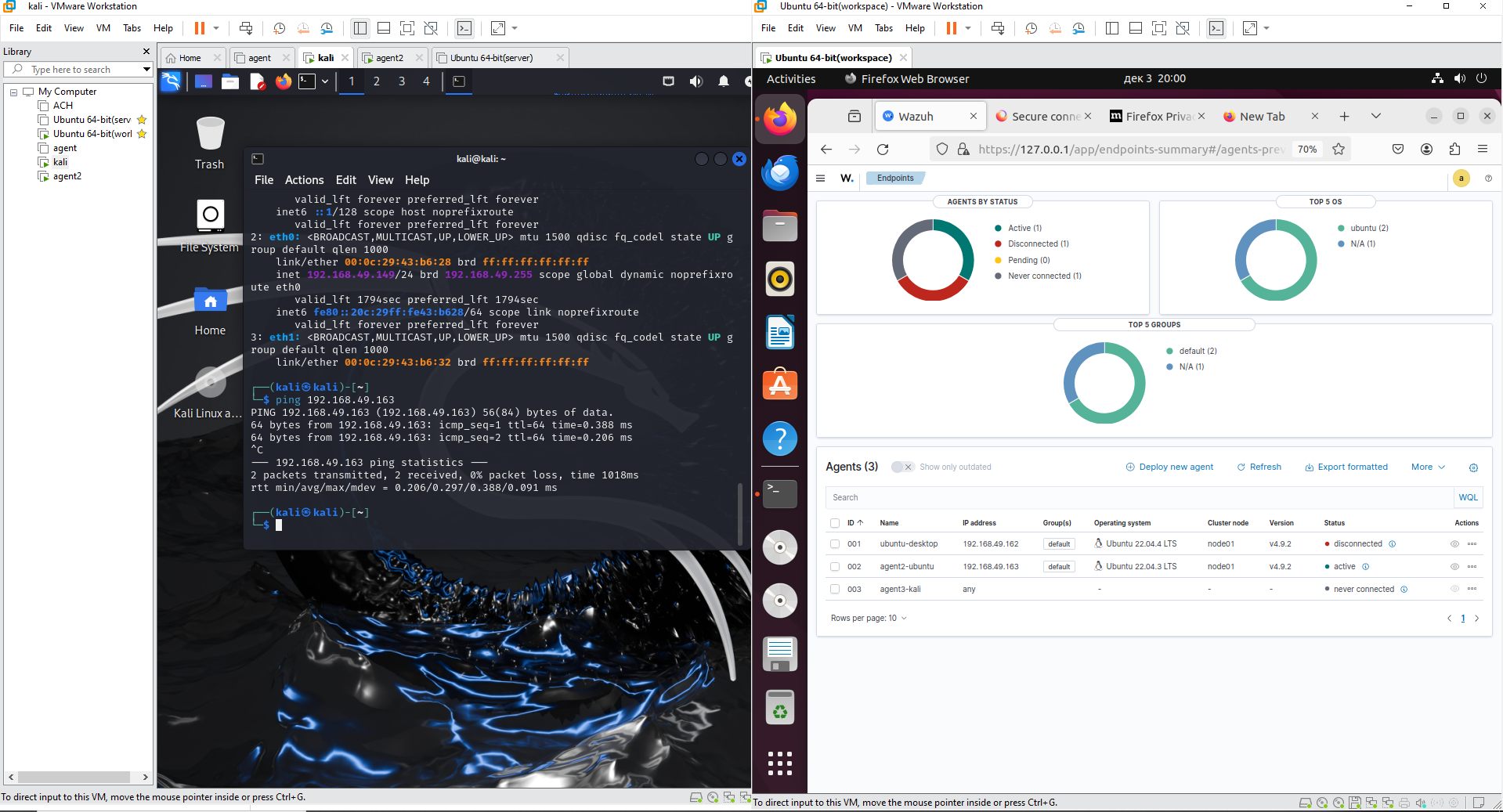
Видим что сервер «увидел» агента

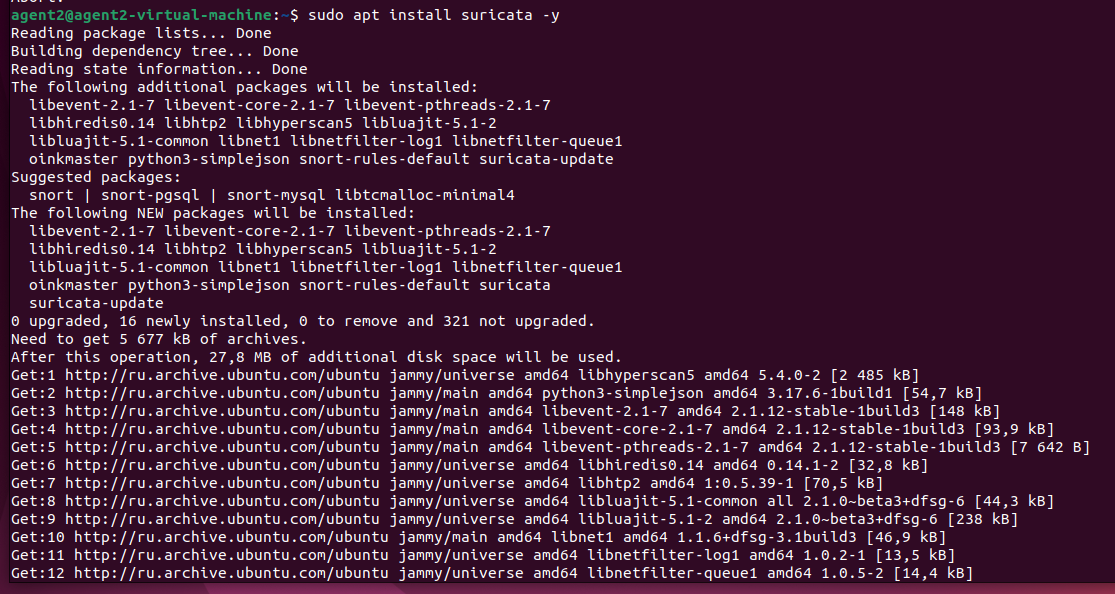
User: admin

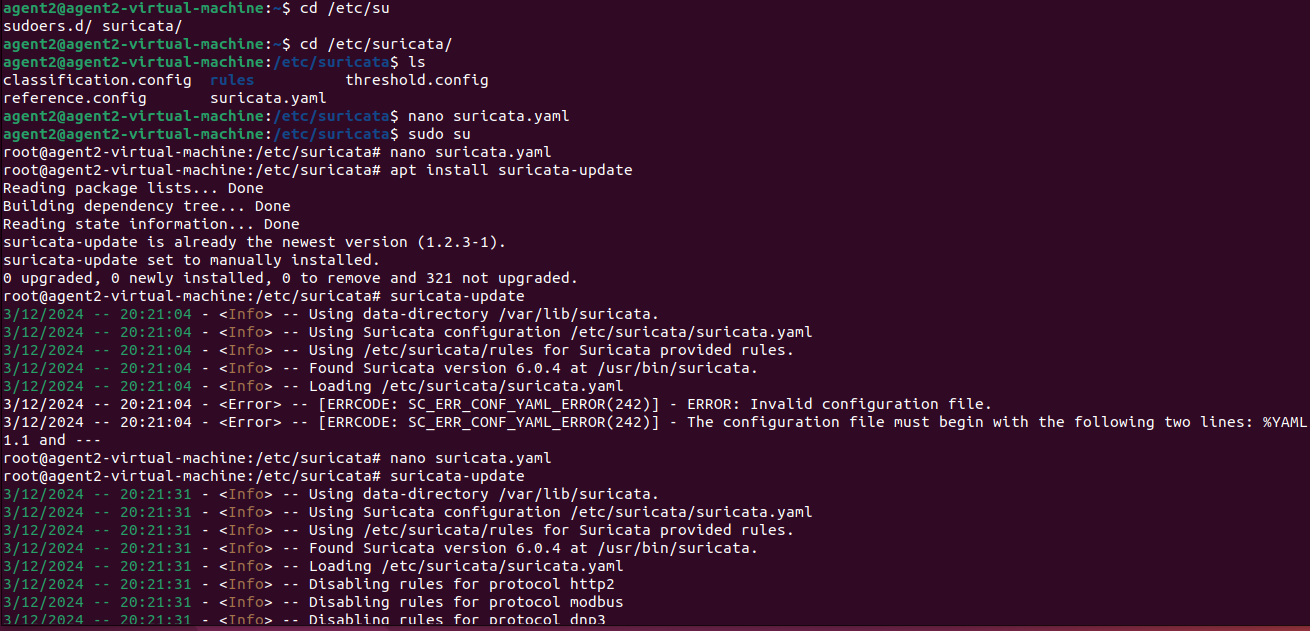
Password: pS4af.kl2SH.zIhc5iv74SRqdvyobiF2

Добавил еще одну машину потому что прошлая почему-то решила больше не работать   


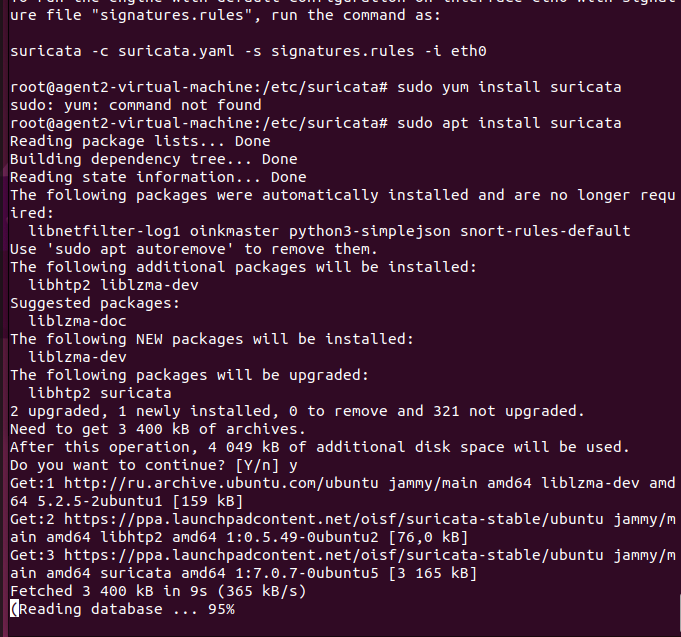
Добавил еще кали линукс,его события тоже можно будет посмотреть

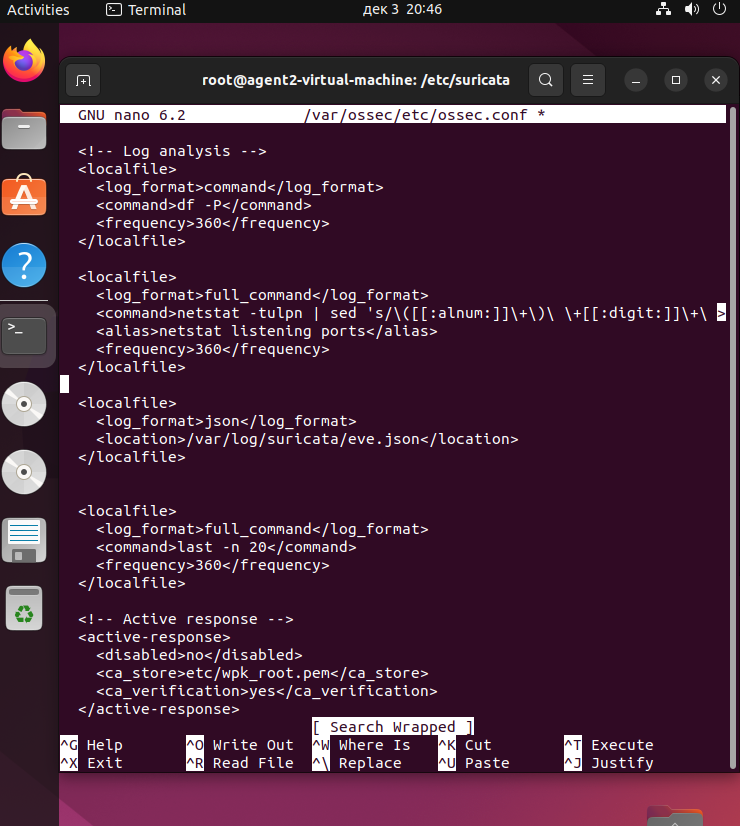


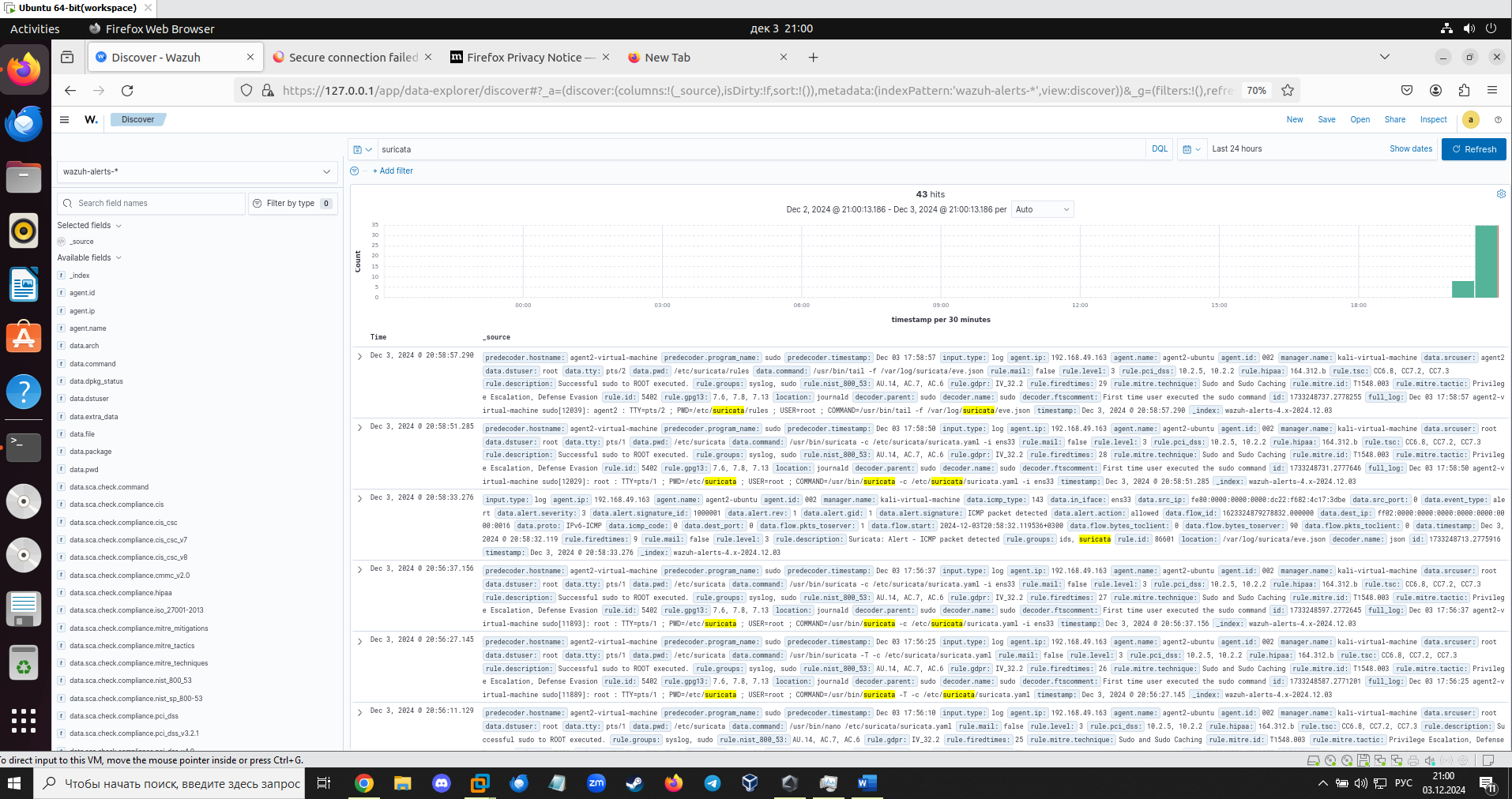
Скачали сурикату  


Установили правила  


Установили на агенте чтобы была интеграция событий с сурикаты в вазух (брал json )

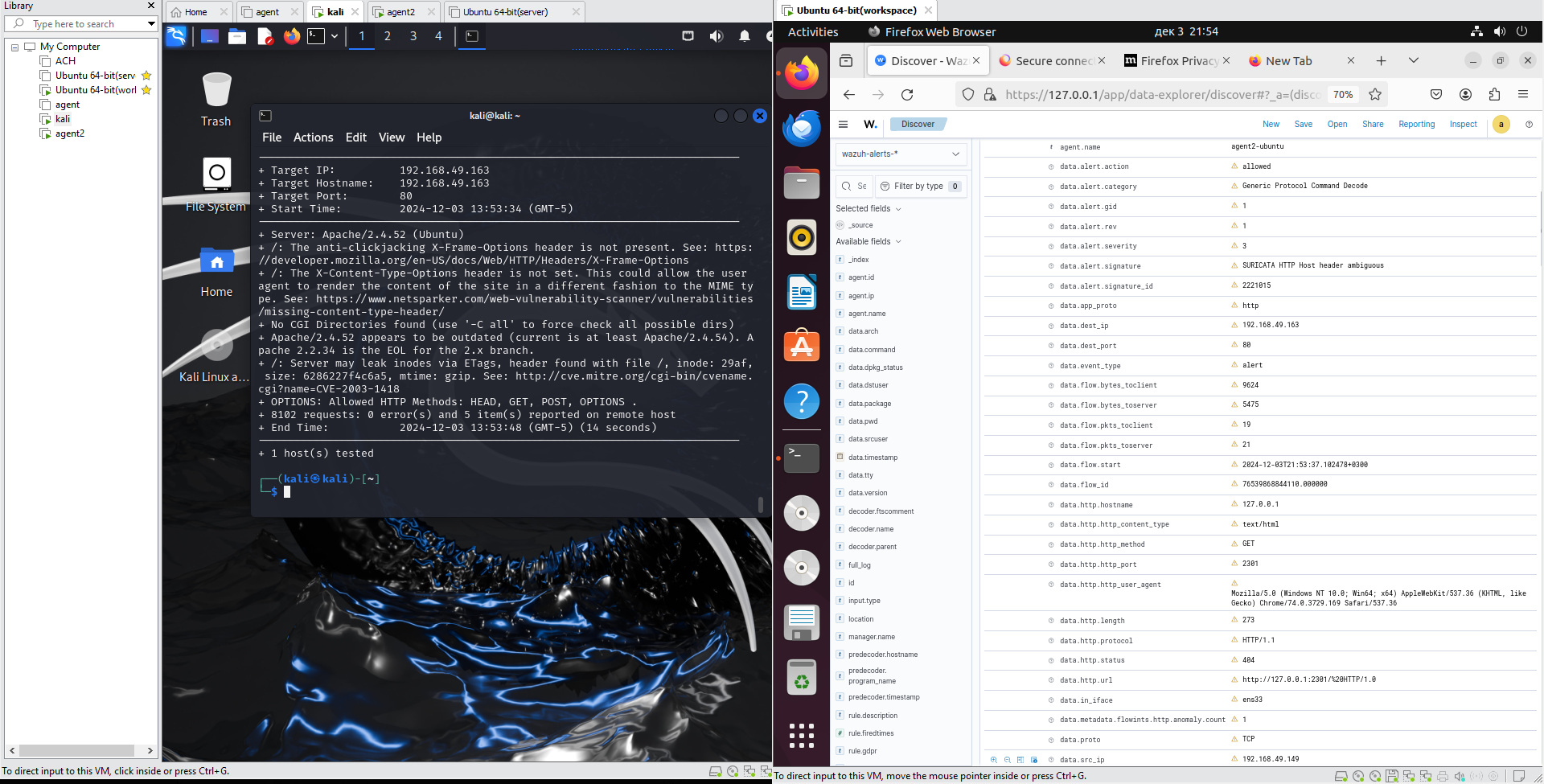
Обновляю сурикату,в связи с многочисленными ошибками  




События приходят в вазух   


Это я отправлял пакет с кали на убунту   


Проверка получения событий





Для интегрирования событий yara

