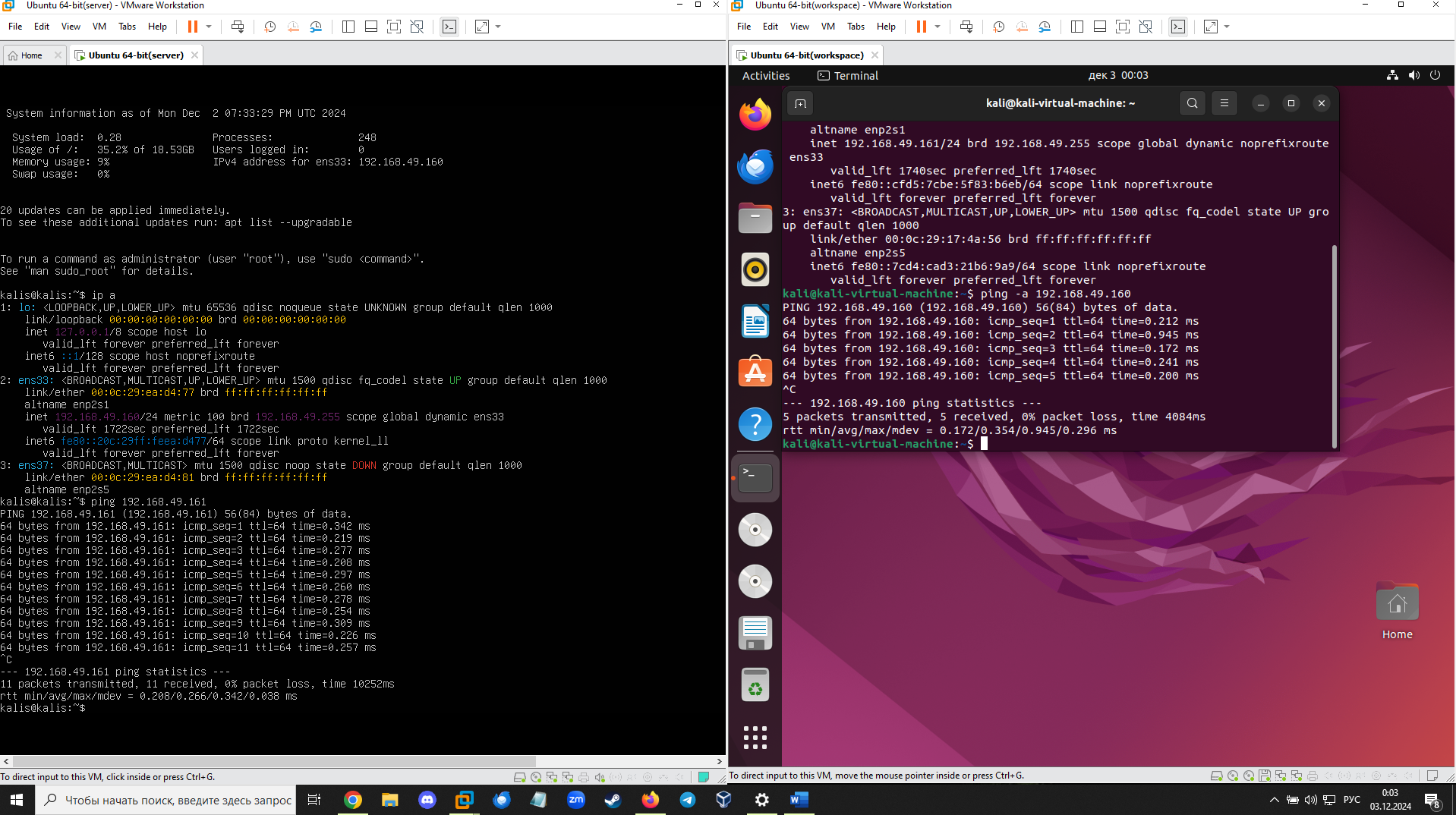
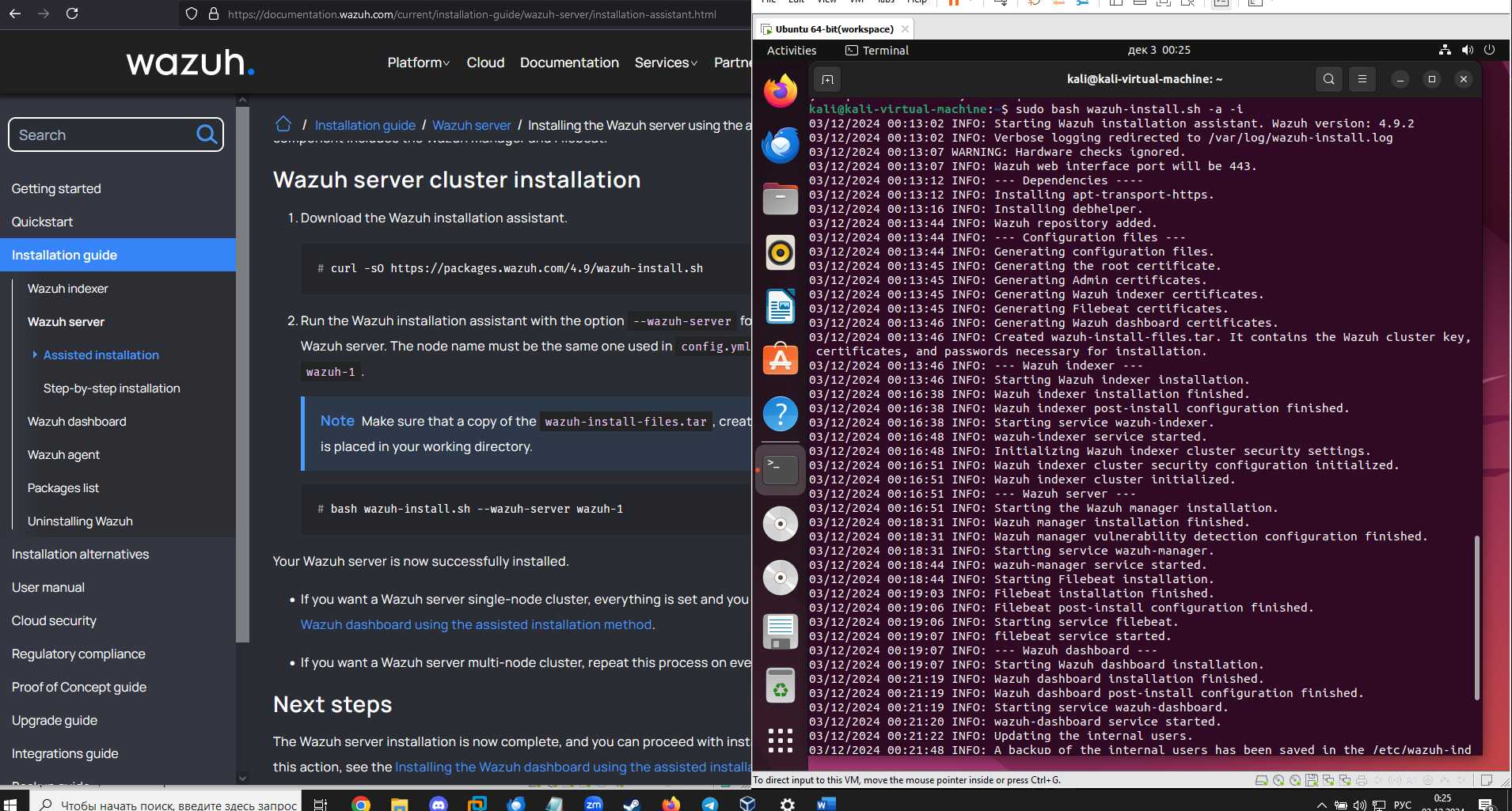
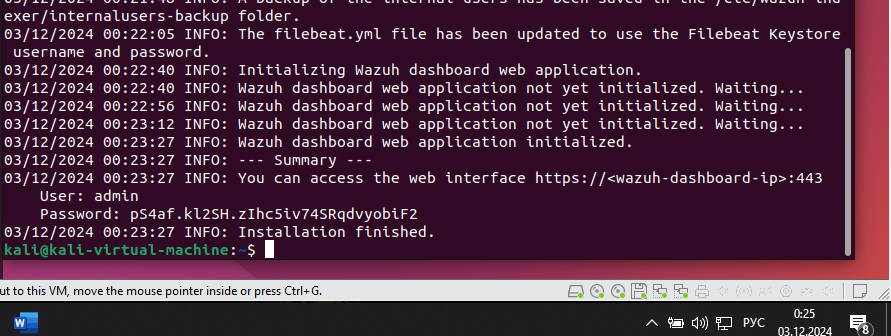
ПРЗ 3. WAZUH.

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



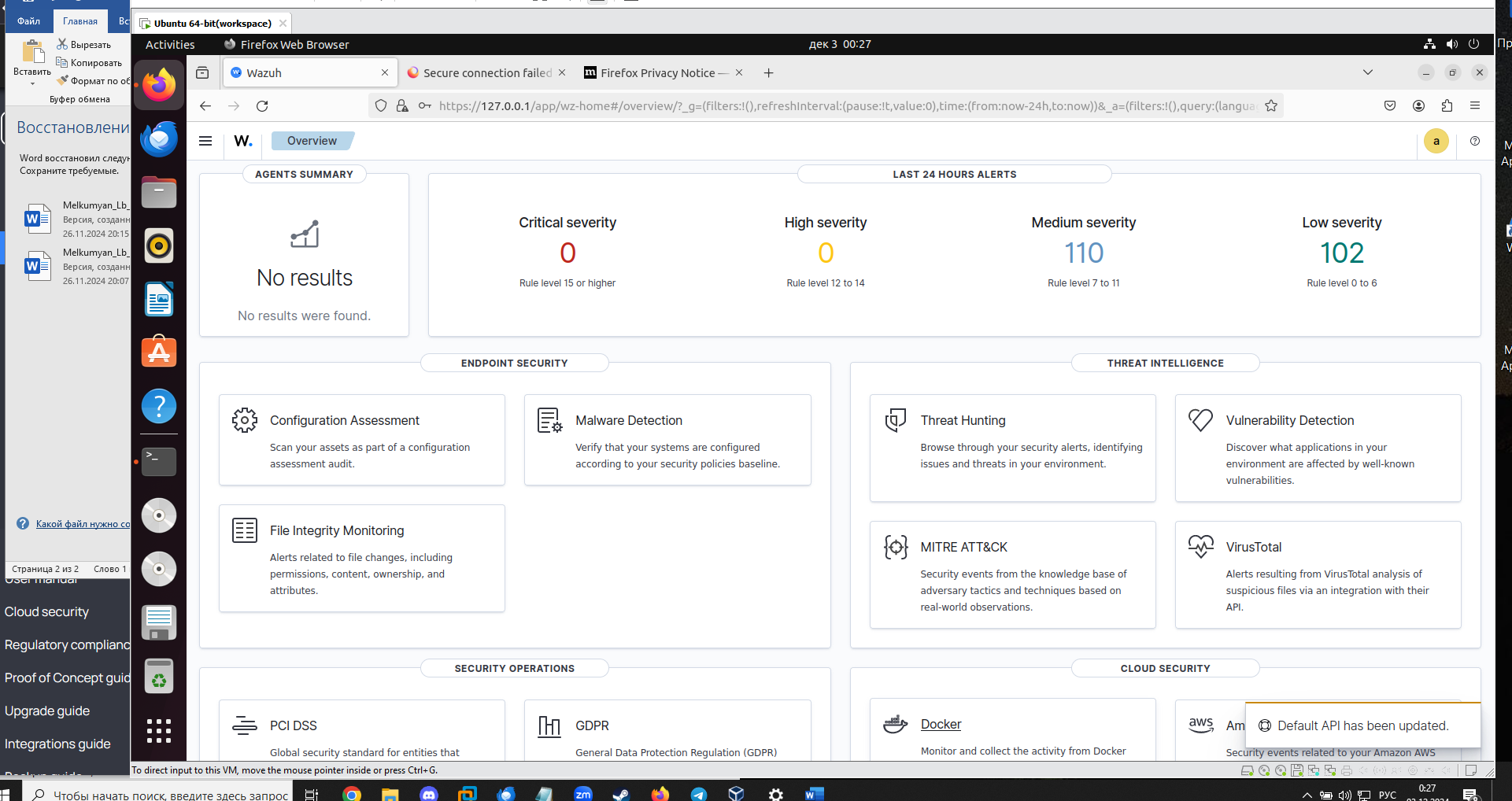
1. Развернуть на одной из ВМ сервер Wazuh



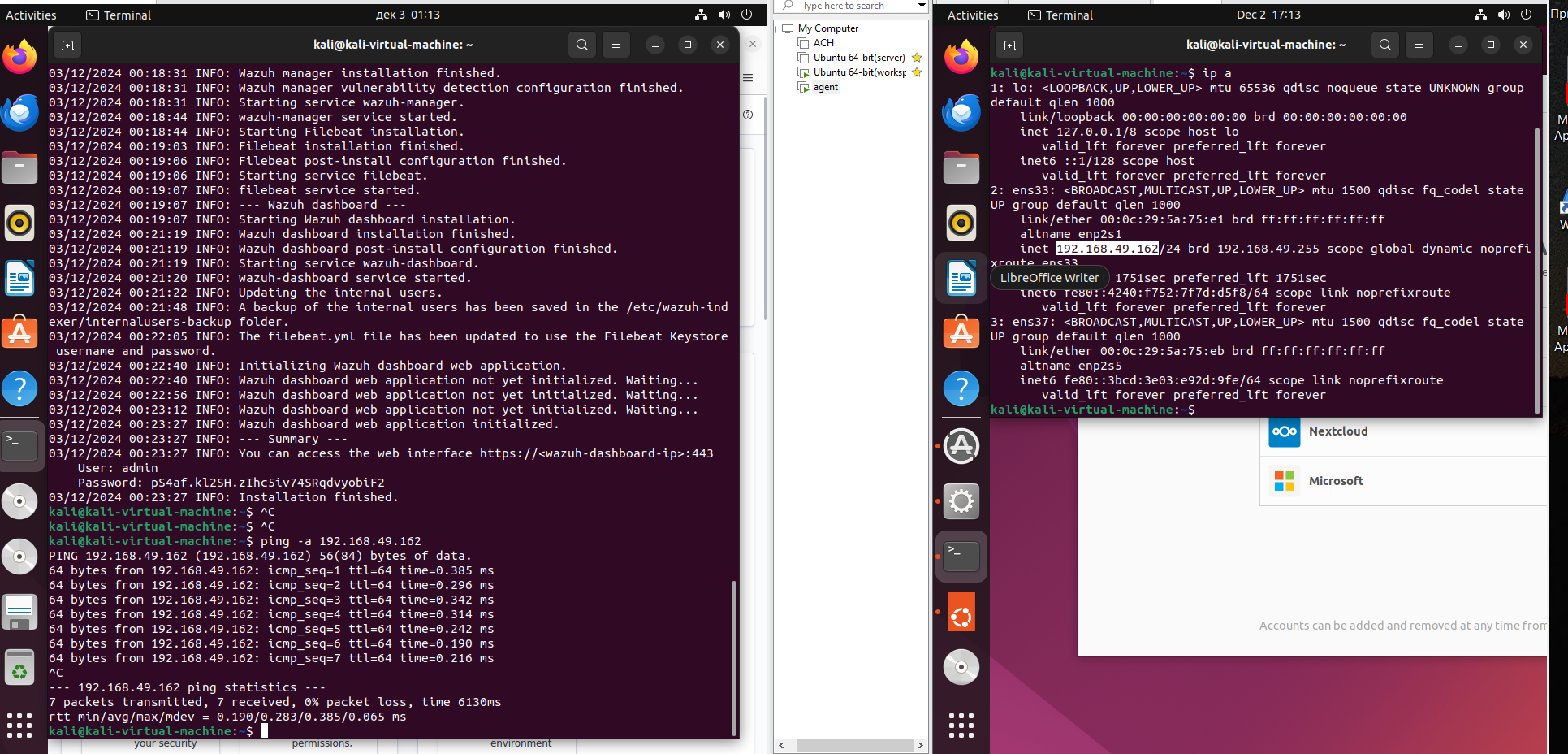
User: admin

Password: pS4af.kl2SH.zIhc5iv74SRqdvyobiF2

Зашли на сам Wazuh

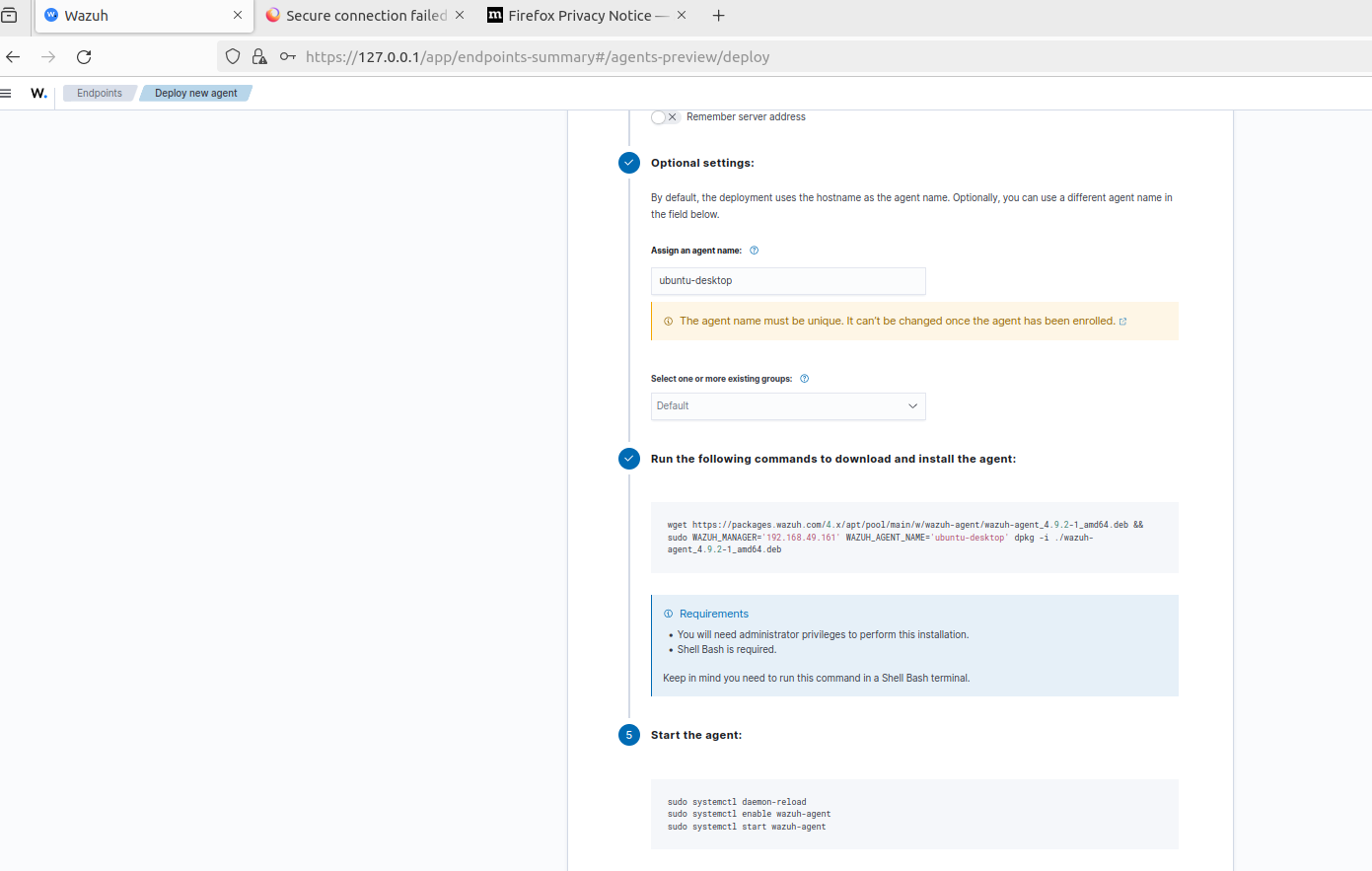


Еще раз проверил сетевую связанность между машинами потому что будучи сонным установил не туда,и пришлось еще одну машину разворачивать

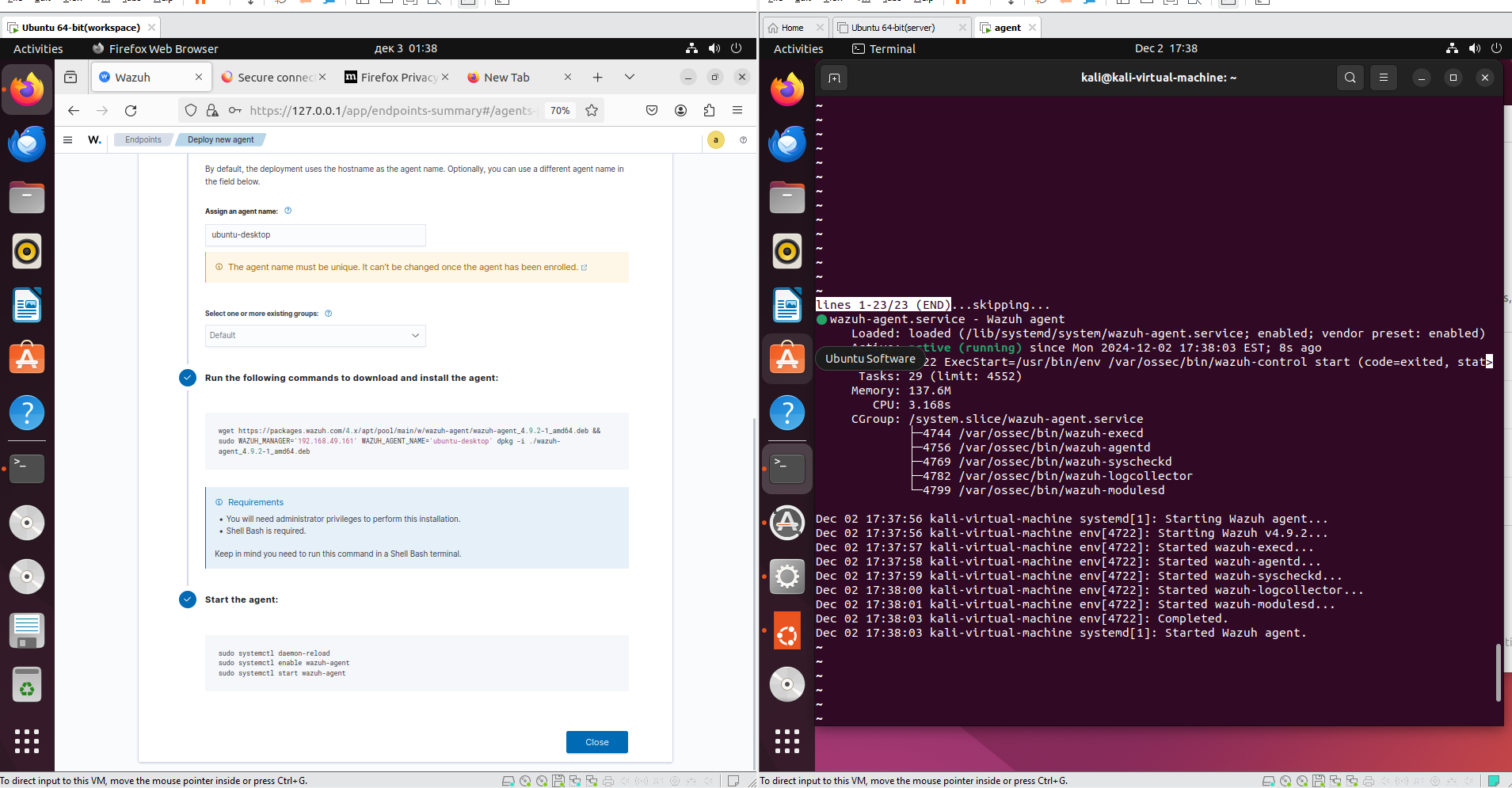


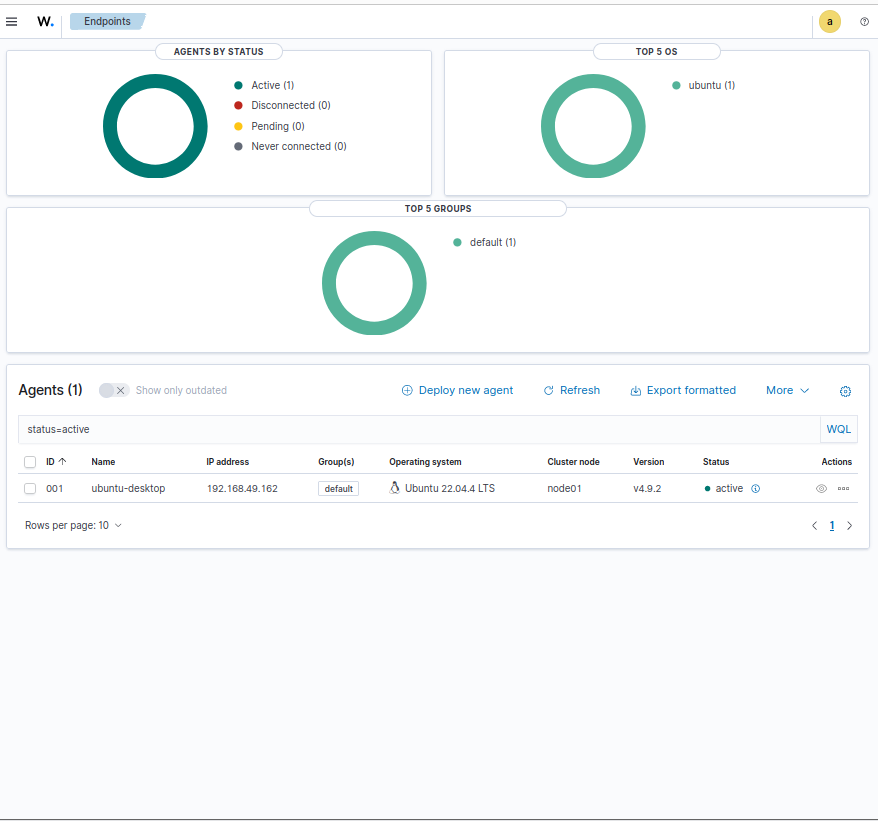
1. Подключите агента используя документацию

Устанавливаю агента через Wazuh



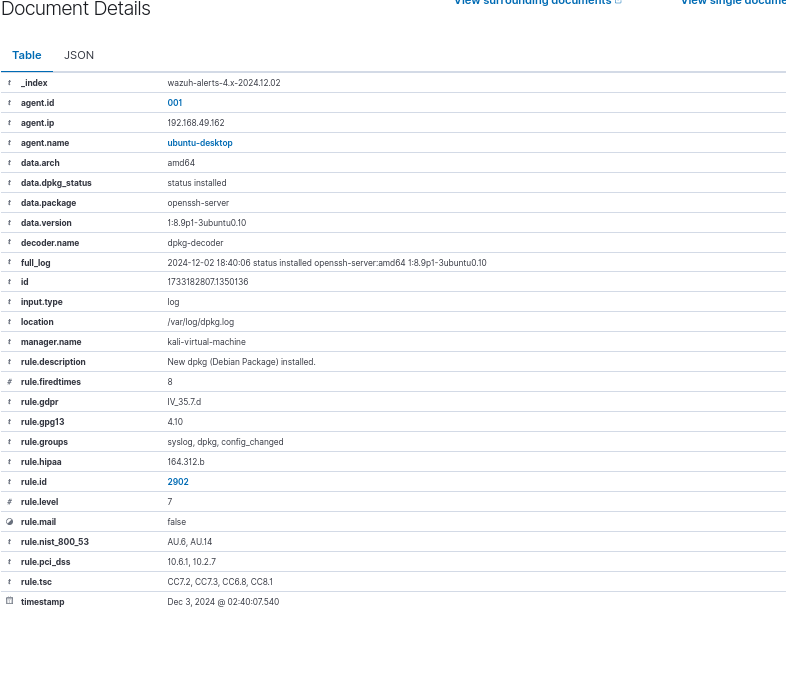
Ввели все команды и установили



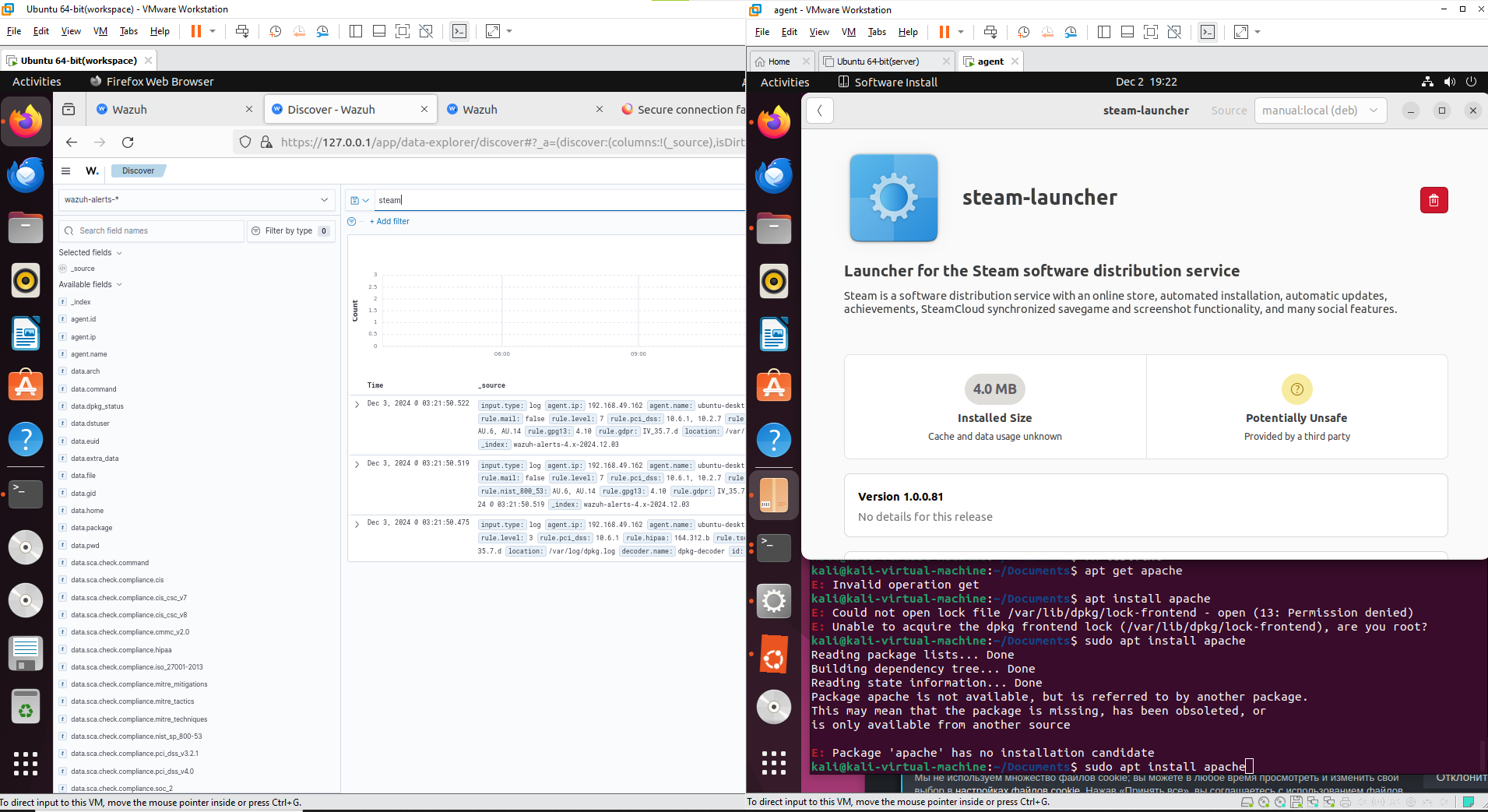
Видим что сервер «увидел» агента  


1. Создайте проверку целостности файлов

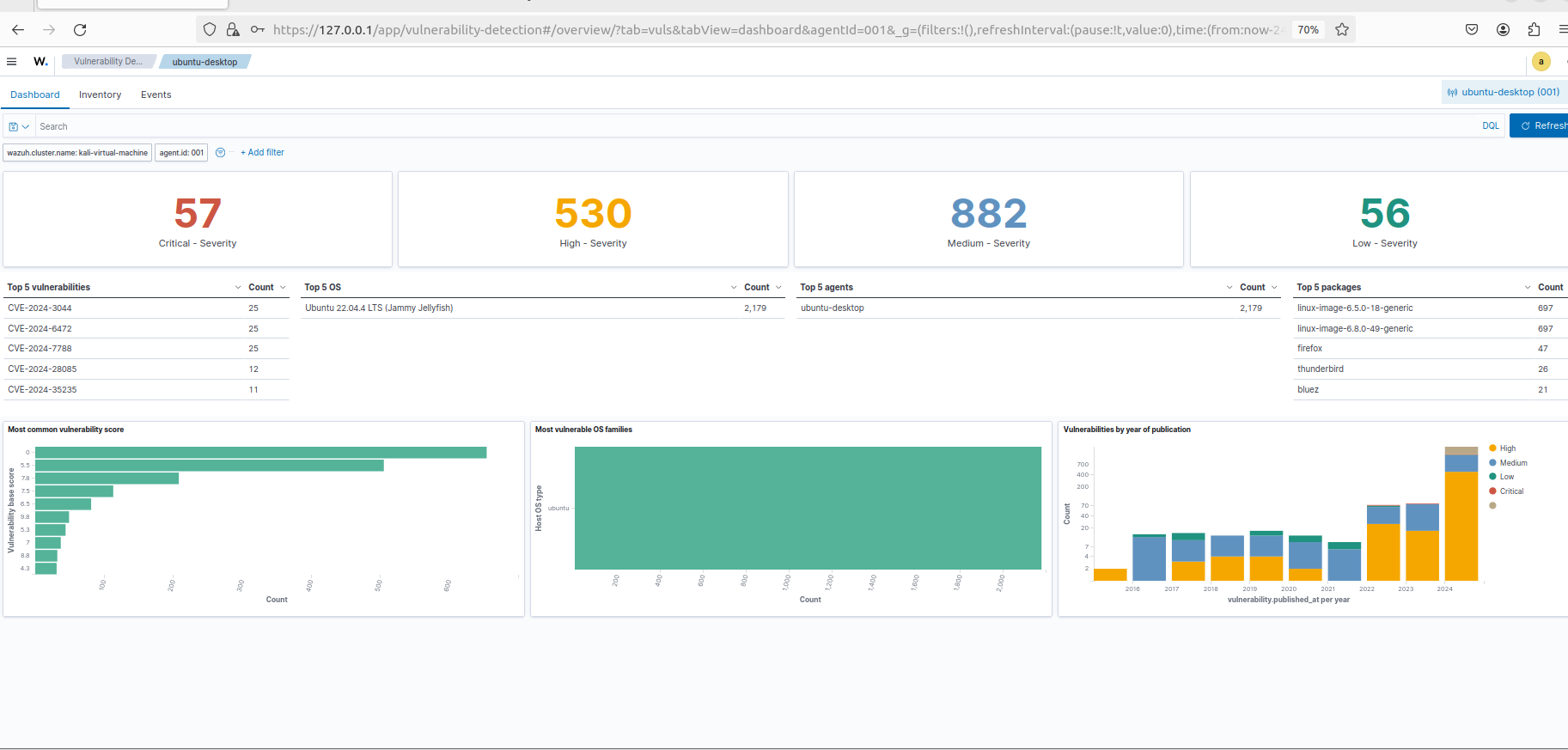
События с файлами приходят



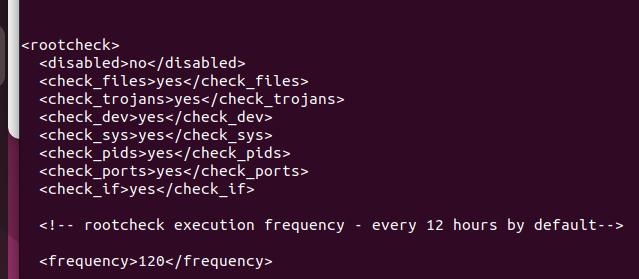
При установке steam поступают события



Настройте выявление уязвимостей в соответствии с документацией



Настройте выявление скрытых процессов



Настройте выявление SQL-инъекций.



Настройте выявление web shell attack.

