**Настройка sshuser'а на всех устройствах кроме FW-DT**

Настройка sshuser выполняется через одну большую команду:

useradd sshuser -m -s /bin/bash -p $(openssl passwd -1 P@ssw0rd) && usermod -aG wheel sshuser && apt-get update && apt-get install sudo openssh -y && systemctl enable --now sshd && chmod +w /etc/sudoers && echo "sshuser ALL=(ALL:ALL) NOPASSWD: ALL" >> /etc/sudoers

Проверка через ssh sshuser@localhost, sudo -i

**Настройка NTP-сервера**

Настройка NTP-клиентов выполняется через одну команду:

echo 'server 172.16.10.66 prefer' >> /etc/chrony.conf && apt-get install glibc-timezones && timedatectl set-timezone Europe/Moscow && systemctl restart chronyd && chronyc makestep

(config) ntp synchronize - команда синхронизации роутера с NTP-сервером.

chronyc makestep - команда синхронизации любого другого устройства с NTP-сервером.

**Настройка Samba (основной DC, добавление DNS-записей, пользователи с группами и подразделениями, резервный DC, ввод клиентов в домен и общая папка)**

<https://dzen.ru/a/ZOUJlubBACmaTby4> (поиск статьи по ключевым словам: alt linux samba dc)

Уточнение! в разделе logging файла /etc/bind/options.conf необходимо прописать следующую строку: category lame-servers { null; };

<https://habr.com/ru/articles/450572/> (поиск статьи по ключевым словам: alt linux samba резервный контроллер)

Уточнение! предварительно на FW-DT отключаем перехват пользовательских DNS-запросов, а также в разделе [libdefaults] файла /etc/krb5.conf меняем значение строки dns\_lookup\_realm с true на false. при вводе команды samba-tool domain join обязательно добавляем ключи —realm=au.team и —dns-backend=BIND9\_DLZ. После присоединения к домену проверяем репликацию с основным контроллером домена с помощью команды samba-tool drs showrepl –summary.

<https://docs.altlinux.org/ru-RU/archive/2.4/html-single/master/alt-docs-master/ch06s14.html> (поиск статьи по ключевым словам: среда интеграции с Windows)

Настройка общей папки в Samba. В конфигурационном файле smb.conf прописываем нужные параметры и задаём им значения yes. После перезагружаем samba и проверяем наличие общей папки: smbclient -L localhost -U administrator.

**Бэкап общей папки через systemctl**

<https://habr.com/ru/articles/540096/> (поиск статьи по ключевым словам: настраиваем restic)

В параметре ExecStart файла backup.service указываем: /bin/tar -czf "/var/bac/SAMBA.tar.gz" /opt/data. В блоке [Timer] файла backup.timer добавляем параметры Persistent и Unit со значениями true и backup.sevice соответственно.

**ADMC**

<https://www.altlinux.org/%D0%93%D1%80%D1%83%D0%BF%D0%BF%D0%BE%D0%B2%D1%8B%D0%B5_%D0%BF%D0%BE%D0%BB%D0%B8%D1%82%D0%B8%D0%BA%D0%B8/ADMC> (поиск статьи по ключевым словам: admc)

На всех устройствах CLI и ADMIN устанавливаем gpupdate и включаем модуль групповых политик через gpupdate-setup enable. На admin-hq устанавливаем admc, получаем билет kerberos через kinit administrator@AU.TEAM через обычного пользователя, заходим в admc, устанавливаем gpui и для подразделения CLI создаём групповую политику Рабочий стол, в которой лезем по пути Компьютер/Административные шаблоны/Система ALT/Настройки Mate/Фон рабочего стола и открываем политику Картинка фона рабочего стола, включаем её, прописываем путь к файлу smb://srv1-hq.au.team/samba/image.png и блокируем данную политику. Дальше лезем по пути Правила Polkit/Ограничения NetworkManager, включаем все политики, меняем значения на No и блокируем их. Проверяем через клиентов CLI.

Дальше лезем по пути /Компьютер/Настройки/Настройки Системы/Сетевые диски и привязываем общую папку через Новый -> Сетевой диск. Действие: Обновить; Путь: smb://srv1-hq/samba; Переподключиться: ставим галочку; Название: samba; Использовать: J:; Показать диск; Показать все диски.

**Docker**

<https://habr.com/ru/articles/279659/> (поиск статьи по ключевым словам: быстрый запуск docker-registry)

Устанавливаем docker-engine, запускаем docker.service, создаём локальный DockerRegistry и проверяем наличие контейнера через docker ps.

<https://habr.com/ru/companies/ruvds/articles/439980/> (поиск статьи по ключевым словам: файлы dockerfile)

Содержимое файла Dockerfile:

FROM - задаёт базовый образ (nginx:alpine);

COPY – копирует с локального хоста в контейнер (index.html /usr/share/nginx/html).

<https://www.dmosk.ru/miniinstruktions.php?mini=docker-self-image> (поиск статьи по ключевым словам: свой образ docker)

Вместо dmosk/nginx:v1 вводим наш образ localhost:5000/web:1.0, проверяем через docker images, загружаем образ, собранный из Dockerfile, в локальный DockerRegistry через docker push <образ>, удаляем образ через docker rmi и загружаем обратно из DockerRegistry через docker pull.

При запуске контейнера Web к команде docker run добавляем параметры --restart=always и --name=web. После запуска контейнера проверяем его наличие через docker ps, доступ к веб-серверу через curl localhost, к приложению - вводим полное доменное имя сервера srv2-dt в адресную строку браузера.

**Настройка Zabbix, добавление узлов в систему, настройка сервера сбора логов**

<https://www.altlinux.org/%D0%A3%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BA%D0%B0_%D0%B8_%D0%BF%D0%B5%D1%80%D0%B2%D0%BE%D0%BD%D0%B0%D1%87%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%BD%D0%B0%D1%81%D1%82%D1%80%D0%BE%D0%B9%D0%BA%D0%B0_ZABBIX> (поиск статьи по ключевым словам: zabbix alt linux)

Полная настройка Zabbix с базой данных PostgreSQL. После создания базы данных перезагружаем postgresql. Перед входом в веб-интерфейс сначала изменяем права доступа к конфигурационному каталогу веб-интерфейса, а уже затем перезагружаем httpd2.

Настройка агента и добавление узлов в Zabbix:

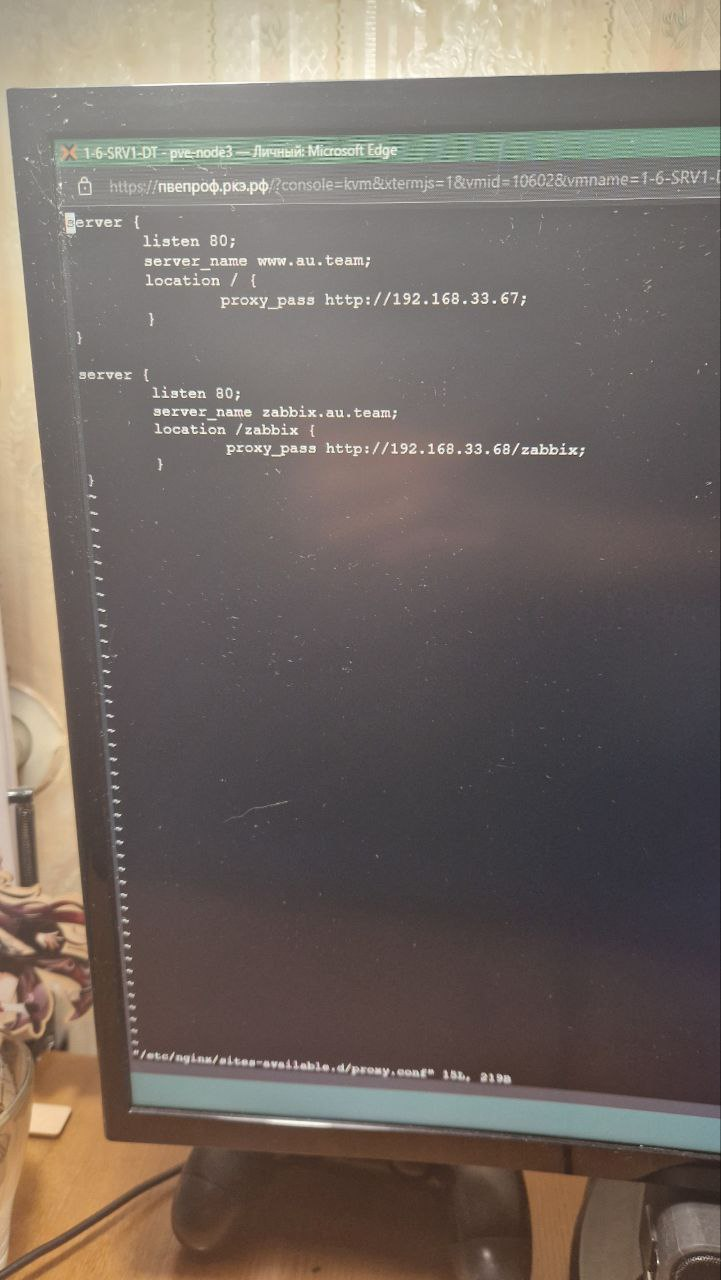
<https://serverspace.ru/support/help/ustanovka-agenta-zabbix-na-ubuntu/> (поиск статьи по ключевым словам: установка агента zabbix)

<https://serverspace.ru/support/help/sozdanie-i-nastroyka-uzlov-seti-i-elementov-dannih/> (поиск статьи по ключевым словам: настройка узлов zabbix)

**Nginx**

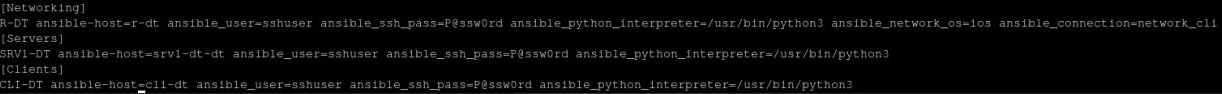
<https://www.nic.ru/help/nastrojka-obratnogo-proksi-nginx_11544.html> (поиск статьи по ключевым словам: настройка обратного прокси)

Настройка веб-сервера nginx как обратного прокси-сервера. конфигурационный файл создаём по пути: /etc/nginx/sites-available.d/proxy.conf. в блок server добавляем listen <порт> и server\_name <доменное имя>, внутри него создаём блок location /, в который вкладываем proxy\_pass http://<IP-адрес;. в блоке server с доменным именем zabbix к блоку location / добавляем zabbix, к proxy\_pass также добавляем /zabbix;. после этого создаём символьную ссылку на созданный файл: ln -s /etc/nginx/sites-available.d/proxy.conf /etc/nginx/sites-enabled.d/.



**Ansible, проверка доступа ко всем устройствам**

Настройка инвентаря ansible: устанавливаем пакеты ansible и sshpass, после назначаем необходимые права на директорию /etc/ansible: chown -R root:user /etc/ansible и chmod -R 774 /etc/ansible. под обычным пользователем переходим в директорию /etc/ansible и создаём файл inventory, в котором прописываем следующее содержимое:



После лезем в файл ansible.cfg, где прописываем путь до инвентарного файла, а также отключаем проверку SSH-ключей на хосте, и уже далее проводим проверку работоспособности через ansible -m ping all.

**Кибер Бэкап (сервер управления, настройка пользователя и организации, агент с функцией узла хранения, настройка на агенте диска и создание плана бэкапа, его выполнение)**

<https://kb.cyberprotect.ru/articles/snapapi-manual> (поиск статьи по ключевым словам: snapapi)

Настройка сервера управления Кибер Бэкап. Сначала обновляем ядро, а уже затем устанавливаем нужные нам пакеты. После обновления ядра очищаем локальный репозиторий от извлеченных файлов пакетов с помощью apt-get clean и перезагружаем систему. Ветка ядра Альт Линукс - std. После обновления ядра и установки пакетов выдаём права на исполнение файлу-установщику и непосредственно запускаем его. При установке компонентов оставляем Management Server и Agent for Linux.

**Настройка пользователя и организации в Кибер Бэкап**. Создаём пользователя wsradmin на уровне ОС, в веб-интерфейсе создаём отдел wsr и добавляем в него созданного нами локального пользователя с правами администратора. Для возможности входа в веб-интерфейс добавляем wsradmin через echo по пути: /etc/security/acronisagent.conf. После этого перезагружаем acronis\_ams и acronis\_asm и пытаемся войти в веб-интерфейс под wsradmin.

**Настройка агента Кибер Бэкап**. Процесс подготовки и запуска файла-установщика аналогичен процессу на сервере управления. В качестве модулей выбираем Agent for Linux и Storage Node.

<https://kb.cyberprotect.ru/articles/registeragent> (поиск статьи по ключевым словам: ручная регистрация агента на сервере управления)

В случае неудачного подключения агента к серверу проводим ручное подключение с помощью следующей команды: /usr/lib/Acronis/RegisterAgentTool/RegisterAgent -o register -a 192.168.11.85 —token <токен>.

<https://www.dmosk.ru/miniinstruktions.php?mini=linux-fstab> (поиск статьи по ключевым словам: автоматическое монтирование дисков)

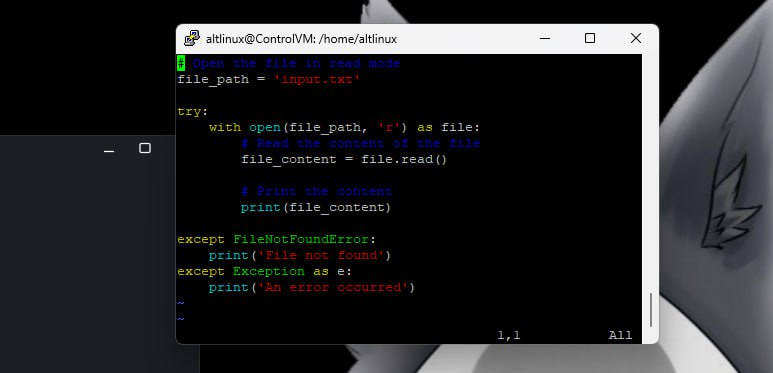
Монтирование диска sdb в директорию backups через /etc/fstab. После добавления устройства в файл вводим команду mount -av.

<https://kb.cyberprotect.ru/articles/286> (поиск статьи по ключевым словам: повторное добавление узла хранения)

В случае неудачной регистрации узла хранения в сервере проведём ручную регистрацию узла с помощью команды: /usr/lib/Acronis/RegisterAgentTool/RegisterAgent -o register -s asn -a 192.168.11.85 -u root -p toor.

**Развертывание приложений в Docker (развертывание Python-скрипта в Docker)**

<https://www.geeksforgeeks.org/print-the-content-of-a-txt-file-in-python/>



**Развертывание приложений в Docker (развертывание WordPress с использованием Docker Compose)**

<https://github.com/froala/wordpress-froala-wysiwyg/blob/master/docker-compose.yml.template>

**Развертывание базового стека ELK**

<https://habr.com/ru/articles/671344/>

**Важные замечания:**

1. Настройку интерфейсов и задание dns-серверов проводим через команду echo.
2. При настройке коммутаторов в файле /etc/net/ifaces/default/options меняем у параметра OVS\_REMOVE значение с yes на no.
3. При настройке STP на коммутаторах: на бриджах добавляем параметр stp\_enable=true, а также other\_config:stp-priority=<приоритет>.
4. (Необязательно) При работе с сертификатом в Ideco скачиваем оттуда корневой сертификат, перемещаем его в /etc/pki/ca-trust/source/anchors. после этого выполняем команду update-ca-trust.