**Руководство администратора по настройке системы резервного копирования**

1. Для развертывания системы мониторинга необходима машина с установленной любым удобным способом ОС Linux и с внутренним IP-адресом 10.128.0.14 и именем bkp2. Данная машина не будет иметь прямой выход в сеть и будет находиться за NAT’ом. Подключение будет осуществляться через машину VPN и monitoring.Еще необходимо создать пару ssh-ключей и обменяться публичным ключом с каждой машиной (vpn, ca, monitoring).
2. Создаем в домашней директории пользователя **user** папку **artefacts**, куда копируем скрипты автоматизации и установочные пакеты.
3. Для развертывания системы резервного копирования необходимо запустить скрипт **backupDeploy.sh** от имени суперпользователя.

Данный скрипт совершит следующие действия:

* Проведет настройку ssh (запретит доступ по паролю, доступ от рута, аутентификацию по паролю и с пустым паролем)
* Установит часовой пояс по Москве и синхронизирует с ним время.
* Установит необходимые пакеты для работы и применит необходимые правила файервола:.

**apt update && apt install -y prometheus-node-exporter iptables apache2-utils**

* Создаст структуру директорий **/home/$bckpUser/backup/**, в которую будут копироваться резервные копии с машин из инфраструктуры
* Создаст файл задачи в крон, по которой после 22 часов в каждый понедельник будут последовательно запущены (исполняемые скрипты) процессы копирования с машин в инфраструктуре.
* Запросит ввести DNS-адреса каждой машины в инфраструктуре. Например ca.ru-central1-a.ru
* Скопирует с машины центра сертификации ключ и сертификат для экспортера прометеус.
* Создаст директорию для экспортера прометеус **/opt/node\_exporter/,** перенесет в нее ключ и сертификат для локального экспортера и корневой сертификат, запросит логин и пароль для подключения к экспортеру (ввести логин admin и пароль), что и будет записано в файл конфигурации **/opt/node\_exporter/web.yml**

- Создаст юнит на автозапуск экспортеров и в конце перезапустит их.