

DevOps: Кровавые капельки опыта

- Деплой в пятницу, да еще и вечером - плохая затея. Очень плохая. Сам не делай и коллегам не давай.
- Поднял любой сервис - настрой лимиты, будь мужиком. Лимиты на CPU/Memory, на кол-во соединений, на все, что в теории может завалить твой сервис. Поверь, коллеги куда как опаснее врагов. Обязательно поломают если давать такую возможность.
- Написал скрипт - проверь его, подробнее тут: [DevOps: Проверь работу скриптов](#). Проверил? Прогони в тестовой песочнице и на тестовых данных.
- Храни скрипты и все нужное и полезное в Git - всегда будешь знать кто и когда вносил изменения, искать крайнего становится неизмеримо легче.
- Бэкапы уже делаешь? 3-2-1? 3-2-1-1-0?
<https://community.veeam.com/blogs-and-podcasts-57/3-2-1-1-0-golden-backup-rule-569> А теперь вопрос: бэкапы тестируешь? Нет? Тогда это не бэкапы.
- Каков RTO (Recovery Time Objective) для восстановления из бэкапа, влазим в SLA для сервисов?
- Храни чувствительные данные в предназначенных для этого местах: Vault, Vaultwarden, KeePass и т.д. Эксельки, текстовые файлы, листики и прочие места где все лежит в открытом виде - это 100% утечка. Разумеется, обновление и патчинг данных сервисов должен быть с повышенным приоритетом. Плюсы - это надежно, проще раздавать и отнимать права, проще отслеживать изменения (и их авторов), проще защищать, не нужно править скрипты.
- Пишите видео сеансов пользователей? Доступ должен быть максимально закрыт. Лично знаю историю как пентестеры получили доступ к видеозаписи сеанса, посмотрели как один из админов копипастит пароли из текстового файла (а потому что буфер обмена был запрещен «для безопасности») и поимели всю инфраструктуру.
- Не делай большие и жирные сервисы - чем больше объем, тем дольше восстановление. Особенно касается файловых серверов. Вытаскивать из бэкапа 20 Тб - это к долгому ожиданию.
- Есть сервера-снежинки? 100% гарантия геморроя в будущем. Меры митигации: etckeeper, бэкапы всего сервера целиком и хотя бы /etc. В идеале - отдельный ансисловый плейбук (роль) для раскатки.
- Случился факап - сообщи коллегам, поставь всех заинтересованных в известность, прикинь примерные сроки. Если со сроками непонятно (а в 95% случаев это именно так) - сообщи контрольный срок когда у тебя появятся новые данные: «Коллеги, упал сервис, ведем восстановление. Примерные сроки неизвестны, более точно сможем сказать через пару часов».
- Важный прод? Дублируй каналы, датацентры, сервисы. Предварительно стоит посчитать что дешевле: потери из-за простоя и потери или затраты на отказоустойчивость.

[devops](#), [experience](#), [опыт](#), [кровавый энтерпрайс](#)

From:
<https://wiki.rtzra.ru/> - RTzRa's hive

Permanent link:
<https://wiki.rtzra.ru/devops/devops-experience>

Last update: **2023/08/09 12:49**



