Переезд в я.Облако

Сказ о том, как в условиях кровавого энтерпрайза переместить продукт из on-prem в облачную среду

MAGNIT

Прошел путь от джуна до DevOps-лида, имею мощные лапищи и полжизни строю отказоустойчивые системы.

Agile-маг, Team-маскот, инфраструктурный архитектор в мечтах и просто хороший человек.

Владимир Пашковский

DevOps из EMM TanderStore

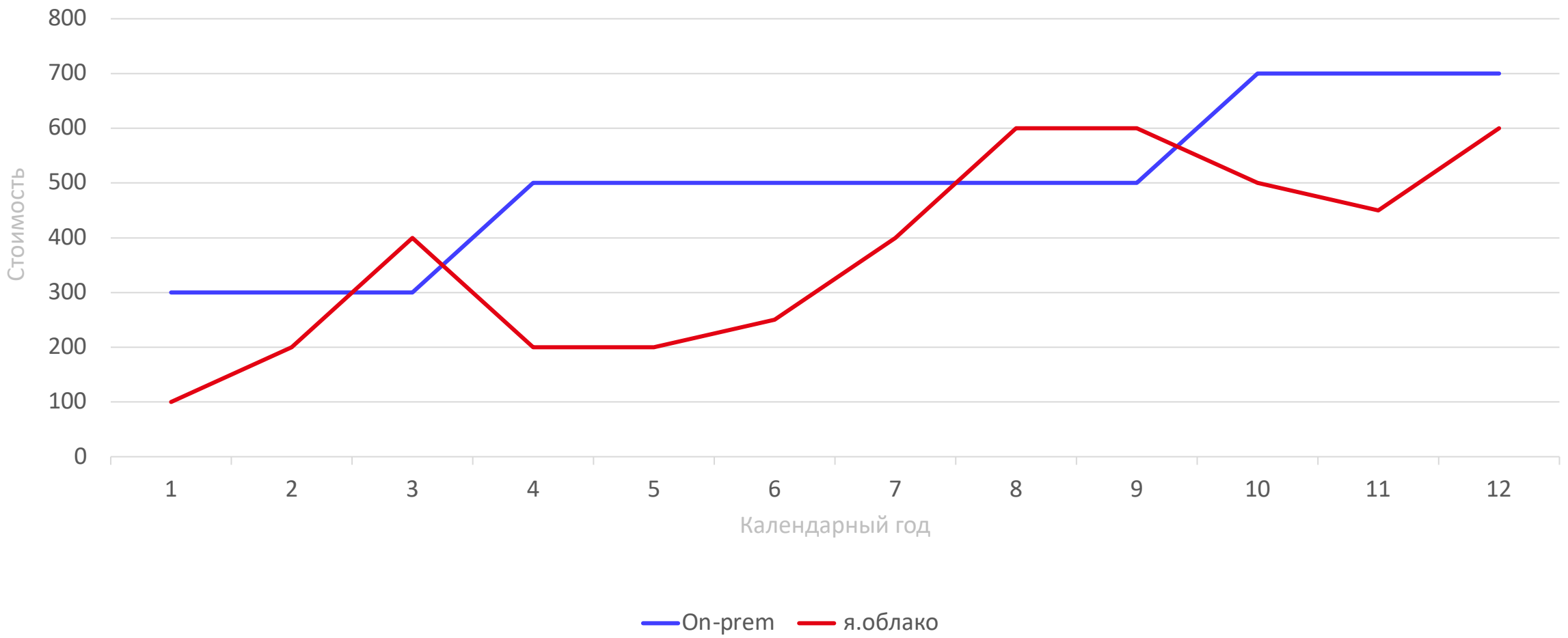
Agenda

- Бюджет
- Ресурсы
- Инфа как план
- Облако настройка
- Легкий старт
- Первая боль
- Проблемы решенные
- Проблемы нерешенные
- Итоги юзера
- Итоги команды

Agenda

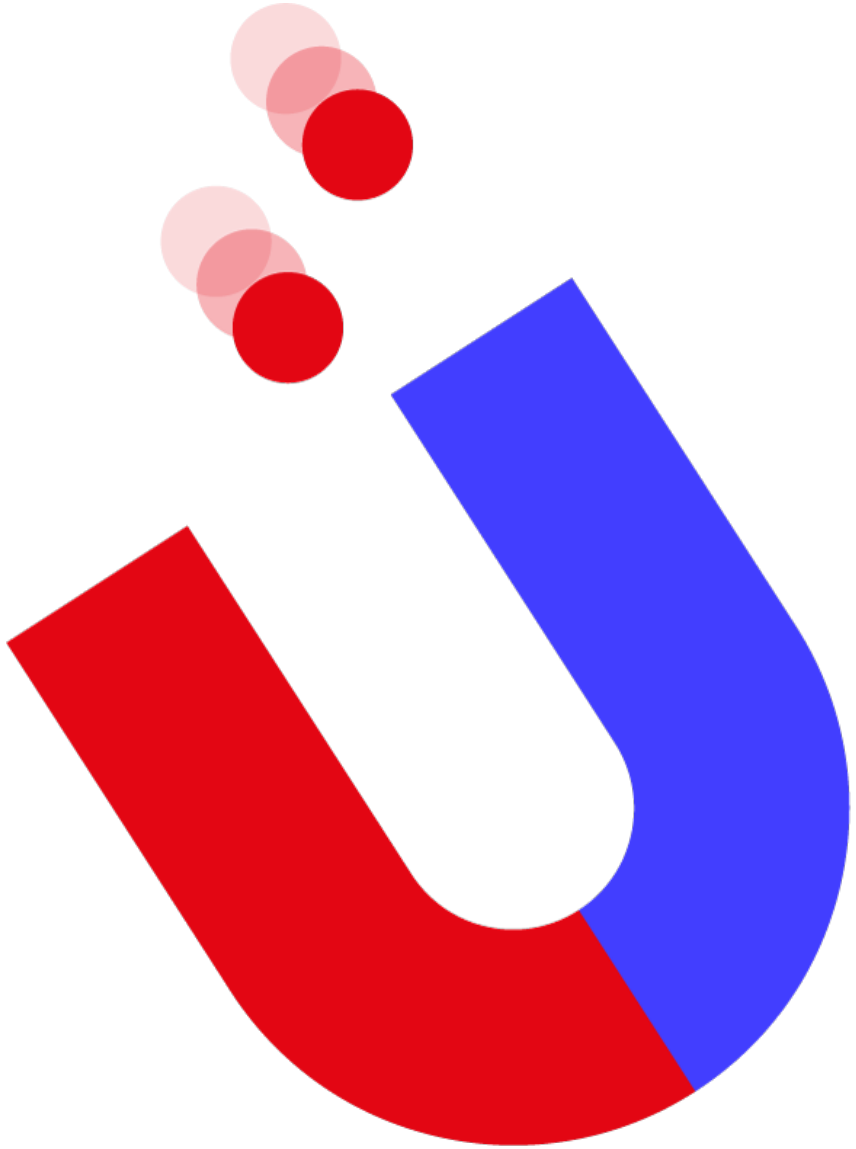
1. Командная подготовка к миграции
2. Легкий старт
3. ~~Проблемы~~ (возможности)
4. Выводы

Бюджет

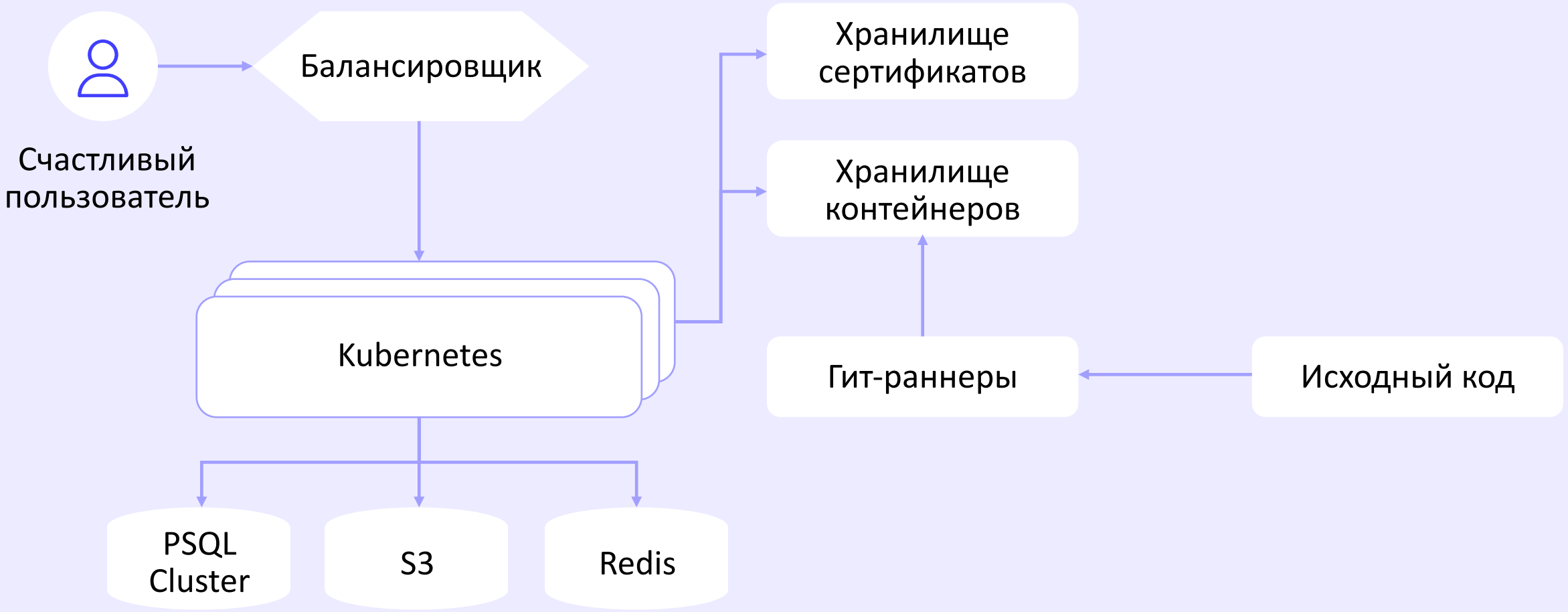

800
700
600
500
400
300
200
100
0
Стоимость
1
2
3
4
5
6
7
8
9
10
11
12
Календарный год
On-prem
я.облако

Ресурсы on-prem vs я.Облако

- NFS – s3
- VM Docker – k8s
- VM BD – Cluster
- (file\ram) Cache – Redis
- Nexus – Container Registry
- VIP – nlb\alb



Инфраструктура, как план



Облако настройка

1. Фолдеры – прод, дев, сервис, что-то, сети
2. Подсети по гео – по 3 на каждый фолдер
3. Группы безопасности
4. Адмнинская BM
5. Служебные аккаунты

Легкий старт

- Целиком – быстро, но больно
- По частям – долго, но не больно

MAGNIT

Первая боль

- Мониторинг
- Логгирование
- Доступно только одно расположение при автоматическом масштабировании
- Managed – это вы
- Публичные ендпоинты
- Оставание в версиях
- Проблемы с правами

MAGNIT

Первые радости

- Прокачка Hard-skillz
- Лицензии (в т.ч. ПД)
- Можно попробовать технологии
- Уровень SLA облака
- Оно работает в два клика!
- Бюджет с запасом
- Свобода действий
- Внутренние сервисы

MAGNIT

Проблемы решенные

Что	Как
DNS облачный + DNS корпоративный не видят друг друга	AD контроллер в облаке Собственный DNS-резолвер
Нет нужных расширений в PSQL Cluster (pg_tap)	Тесты проходят на BM (пайплайн, все дела)
Расписание бекапов только по дням	Cronjob\scheduled + репликация БД
Мониторинг и логирование	3 строчки helm charta
Helm-чарт некуда засунуть	Пуш контейнера+пуш архива
Нет экспертизы со стороны юзера	Время лечит (:
Недостаточная система прав	IaC + толика страданий

Проблемы нерешенные

Инфраструктура
S3 RWX – отваливается mount
Managed postgres ушла в failed state
Ноды k8s могут просесть по производительности
Зеркала YC не всегда доступны

Сервисы
Документация (tf)
Сервисный аккаунт на ВМ в облаке
Права на облако изменяются, нет градиентных ролей
Зеркала YC не всегда доступны

Прочее
Саппорт ((:
Мониторинг операций в облаке не раскрывает суть операции

Итоги, как юзера

PRO	Contra
Managed сервисы не нужно обслуживать	Уровень предоставления Managed сервиса не полный
Существуют готовые решения	Недостаточная опциональность готовых решений
Легко поднять и масштабировать продукт	Нет замечаний (:
Стабильность и SLA зависит от провайдера	Стабильность и SLA зависит от провайдера
Дешевле обслуживание инфраструктуры	Необходим определенный уровень hard-skillz
Готовые лицензии	Некоторое лицензирование невозможно
Технологический рост продукта	Не заглянуть под капот технологий

В целом, плюсы перевешивают и количественно, и качественно. Однако облако требует более тонкого и продуманного подхода.

Итоги, как команды

PRO	Contra
Меньше потребность в сотрудниках поддержки	Сотрудников придется куда то деть. Например поднять hard-skillz
Лицензии (ПД)	
Возможно лучшая ИБ, в контексте доступа снаружи	Проверки исходников по умолчанию нет
Возможно выше уровень поддержки сервисов	Возможно!
SLA\доступность	Зависит от hard-skillz команды и компании в целом

В целом, плюсы перевешивают и количественно, и качественно. Однако облако требует более тонкого и продуманного подхода.

Спасибо за внимание!