????? ???????? ?? ? ?????????????

Каждая новая ВМ при ее создании в PVE проходит ряд этапов:

1. Описание для администратора:
    1. Обновление комплекса технических средств (таблица КТС) в NextCloud - она **доступна тут**); // Выгрузить КТС в NextCloud
    2. Обновление инфраструктурной схемы.
2. Настройка окружения:
    1. Прогон скрипта для автоматической настройки хоста;
    2. Регистрация ее в NetBox;
    3. Сохранение секретов в Hashicorp Vault (даже в случае, если автоматизация в любой форме к ней не применима);
    4. Создание A-записи в доменной зоне DNS (на домен-контроллере);
    5. Проверка работоспособности. // Настроить пайплайн
3. Добавление ВМ в мониторинг. // Настроить пайплайн

Рассмотрим каждый из этих этапов отдельно.

???????? ??? ??????????????

Первым делом, до или после заведения ВМ, необходимо обновить комплекс технических средств (таблица КТС). Она доступна как локально, так и **тут, в NextCloud**. Вносить хост можно по аналогии с уже существующими записями - за все время существования проекта это - наиболее оптимальный формат, к которому я пришел через пробы и ошибки.

После чего нужно **обновить инфраструктурную схему** на **сайте**. Она существует в репозитории самого сайта, но туда попадает только конечный вариант в формате SVG:

1. Схема редактируется через DrawIO локально;
2. Она обезличивается (удаляются IP-адреса, которые определены в WAN);
3. После чего схема экспортируется в формате SVG и загружается в **репозиторий GitLab**.

> Обновление структуры сайта (в том числе, схемы) - автоматический процесс. Достаточно только коммита/Pull-Request в ветку Main, а все остальное сделает

> пайплайн Gitlab-CI.

Делается это по той же причине, по которой заполняется таблица КТС. Такой подход позволяет понимать что и где расположено, а так же, быстрее решать проблемы инфраструктуры в случае чего.

> По сути, это полноценный релизный процесс, только здесь публикуется не ПО или сервис, а сама ВМ.

?????? ??? ?????????????? ????????? ??

Вот вы создали ВМ в PVE и подключились к ней по SSH. Что дальше?

А дальше - первичная настройка. Это первый шаг настройки любой ВМ в моей инфраструктуре. И он включает в себя несколько этапов:

1. Синхронизация времени
2. Установка последних обновлений пакетов
3. Настройка SSH:
    1. Генерация пары из открытого и закрытого ключа
    2. Настройка основного конфигурационного файла SSHD
    3. Применение изменений
4. Расположение TLS-сертификатов для веб-сервера (даже если они не будут использоваться на этом хосте) и применение прав доступа к ним
5. Установка набора ПО по-умолчанию

Все эти этапы можно выполнить вручную, но у любого администратора с таким кол-вом сервисов быстро задергается глаз. Особенно с учетом того, что эти действия иногда приходится выполнять ни один раз. Поэтому для этого действия существует скрипт, который прогоняет все необходимые этапы автоматически. Его достаточно просто скопировать и выполнить на хосте.

> И да, этот скрипт не будет тут указан, потому что он хранит некоторую конфиденциальную информацию. Например, листинг конфигурационного файла SSHD. Где он расположен знает только администратор и лишь ему позволен доступ к нему.

NetBox ? ?????? ?????

Зачем он нужен? В моей инфраструктуре принят принцип описания каждого нового хоста (ВМ), которая вводится в эксплуатацию. Для этого я поднял сервис, который называется NetBox. Он доступен по адресу **netbox.elijahkamsky.ru**.

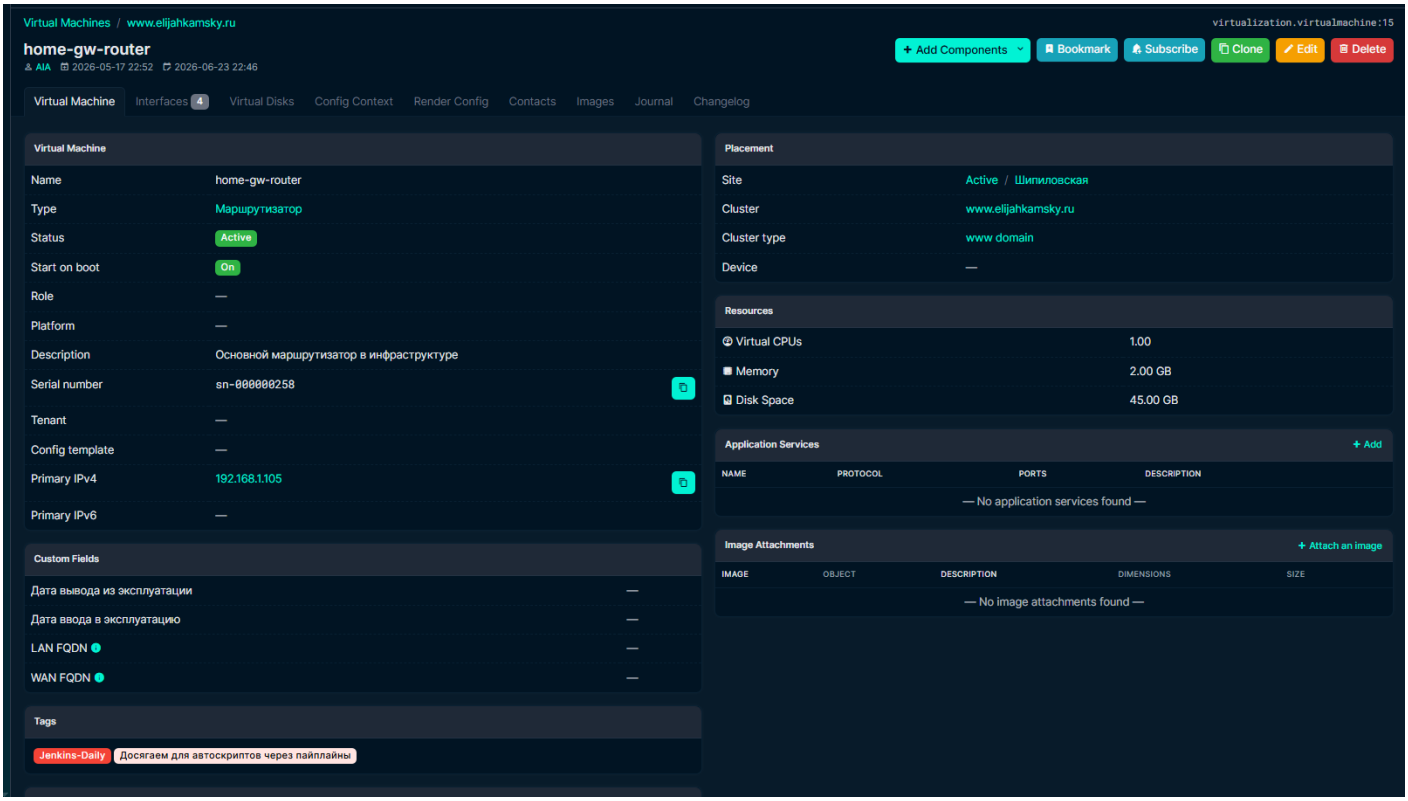
Его задача - хранить описание всех ВМ, чтобы отвечать на вопросы:

1. Что это за ВМ?
2. Какие у нее параметры?
3. Где она находится и к чему принадлежит?
4. Зачем она нужна?
5. С какими сервисами она связана?
6. Какая у нее критичность?

Все эти вопросы берет на себя NetBox. **У описанной ВМ есть:**

1. Название
2. Список сетевых интерфейсов и IP-адреса
3. Серийный номер
4. Домен
5. Описание
6. Ресурсная конфигурация
7. Роль
8. Расположение
9. Владелец
10. Теги (как раз они используются в сценариях автоматизации)
11. Принадлежность к кластеру и/или группе служб
12. Статус активности хоста в данный момент

> Конкретно по статусу активности хоста. Заполняется в т.ч. и информация о его запуске при перезагрузке ноды PVE. Делается это потому, что некоторые хосты описаны, но еще не были введены в эксплуатацию, а некоторые используются ситуативно и поэтому запускаются вручную.



?????-???????????

Для каждой ВМ так же создаются А-записи на домен-контроллере (MS-AD). DNS-сервер, который на нем расположен, содержит полный список имен серверов, включая те, которые только запланированы, но еще не были введены. У ВМ этом может быть много доменов, но каждый из них там перечислен.

> Хост может быть определен сразу в нескольких доменных зонах, если он имеет там IP-адрес. Например, такие записи имеет хост home-admin-ntopng.

Например, у меня есть приложение home-srv-jitsi01 с адресом 10.10.10.22. Вдобавок, оно является публичным сервисом, доступно в WAN. Поэтому оно будет иметь наиболее полный список DNS-записей (за исключением, почтового сервера - но то скорее частный случай). **Конкретно в этом случае, список DNS-записей на DC будет выглядеть примерно так:**

Значение А-записи	Доменная зона	IP-адрес	Описание
home-srv-jitsi01	homeserver.ru	10.10.10.22	Полное наименование хоста в этой доменной зоне

jitsi01	homeserver.ru	10.10.10.22	Короткое наименование хоста в этой доменной зоне. Другие сервисы часто используют именно его
jisti	homeserver.ru	10.10.10.22	Единая точка доступа к сервису указывающая на хост в **LAN**
jisti	elijahkamsky.ru	[WAN-IP]	Единая точка доступа к сервису указывающая на хост в **WAN**

> Конкретно для зоны elijahkamsky.ru настроено делегирование на DNS-сервер провайдера, потому что приоритетным DNS-сервером для ВМ обычно является внутренний домен-контроллер, но он может не хранить какие-то записи, которые уже есть на сервере провайдера.

Hashicorp Vault ? ??????? ???????????

После того, как хост занесен в NetBox и настроены DNS-записи, нужно описать секреты, которые к нему относятся. Как минимум, для каждого хоста это настройки подключения к нему по SSH.

> Да, в идеале на любой хост после его развертывания можно попасть только имея SSH-ключ. Я уже упоминал это, когда говорил про скрипт для автоматической настройки хоста.

Hashicorp Vault расположен по адресу **vault.elijahkamsky.ru** и имеет свою структуру секретов. Но общепринятый путь к хранению секретов там один - Secrets/ssh-secret/ssh/hosts . В этой директории расположены секреты для конкретных хостов. Из прошлого примера, файл назывался бы home-srv-jitsi01.

А теперь к его содержимому. Каждый хост имеет минимум эти поля:

Номер	**Название поля (строго как тут)**	**Описание**
1	name	Hostname ВМ. Это поле часто используется в различных пайплайнах, и именно поэтому шаг с настройкой DNS на домен-контроллере крайне важен

2	host	IP-адрес хоста. Тут больше для информации и как резервный путь доступа к хосту
3	port	Порт для подключения по SSH. Да, обычно он не меняется, но порой порт отличается от значения по-умолчанию. Как раз это поле уточняет связанным системам наличие нюанса
4	username	Имя пользователя для подключения к хосту по SSH
5	private_key	SSH-ключ, который используется для подключения к ВМ

> Помимо этих полей там может храниться еще что-то - тут все зависит уже от конкретного назначения ВМ.

> **Каждое поле из указанных обязательно должно быть заполнено!** Без этого не будет работать часть автоматических задач, включая обновление ВМ и синхронизации, а так же не будет возможности в целом подключить ВМ к пайплайнам в Jenkins

???????? ??????????????????

Как проверить, что все работает правильно?

По сути, единственное что реально влияет на работу системы - это NetBox и Vault. Остальное - исключительно удобство администратора. Поэтому проверку можно проводить сразу, как только эти 2 шага выполнены. И ответ на вопрос прост: вот **этот Jenkins-pipeline**, который это верифицирует.

Настройки пайплайна включают только сам хост (или хосты). Укажите их в списке хостов и запустите пайплайн.

В логах вы увидите явный вывод: верно ли вы настроили систему. При наличии проблем, по выводу так же можно понять, что именно и почему не заработало. Первостепенная задача администратора - сделать так, чтобы пайплайн завершился без ошибок на новом хосте.

> Стоит уточнить, что это **идемпотентный** пайплайн. Т.е. это пайплайн, который можно запускать сколько угодно раз с одинаковыми входными данными, и после первого успешного выполнения состояние системы больше не изменится.

?????????? ?? ? ??????????

> К этому шагу можно переходить только в случае, если пайплайн из предыдущего шага завершился успешно!

Если с предыдущими шагами проблем более не возникает, можно переходить к настройке мониторинга. Тут точно так же, как и в случае со скриптом автоматической настройки, есть свои стандарты. Минимум, что должно мониториться на каждом хосте - метрики самого хоста (ЦПУ / ОЗУ / Дисковое пространство и т.п.).

Конечно, вы можете сделать это вручную. Тут ничего сложного нет. И да, как вы могли догадаться, - и здесь тоже есть свой пайплайн. В очередной раз. И он тоже идемпотентен

Что конкретно он делает?

1. Берет имя хоста, который требуется добавить в список мониторинга
2. Проверяет, есть ли этот хост в мониторинге или нет
3. **Если хоста в мониторинге пока что не появлялось**, он:
    1. Зайдет на хост и установит Prometheus-node-exporter;
    2. Добавит хост в цели для мониторинга Prometheus;
    3. Зальет обновленный конфиг в ветку этого репозитория (чтобы администратор мог удобно изменить его вручную).
4. **В противном случае** вы получите предупреждение о том, что хост уже добавлен в мониторинг.

После чего, вы сможете проверить состояние хоста в **системе мониторинга**, в дашборде PNE 25.06.2026.

> Метрики собираются автоматически, но **аллертинг по утилизации ресурсов в этой схеме пока не предусмотрен**!

??? ????????? ?????????

Перед добавлением хоста нужно задать всего одну настройку - полный домен новой ВМ.

Помните пример с home-srv-jitsi01? Не просто так мы настраивали DNS-записи. В этом примере мы создавали A-запись в домене homeserver.ru, следовательно прописывать нам нужно именно **home-srv-jitsi01.homeserver.ru**.

>

> Будьте внимательны! Прописывать полный и правильный домен здесь критически важно - от этого зависит качество мониторинга.

Пайплайн так же поддерживает добавления множества хостов - достаточно прописать их в соответствующем окне, **по 1 на строку**.

????? ?? ????????? ????????? ? ?????????????

ВМ считается введенной в эксплуатацию **только если**:

1. NetBox содержит описание ВМ
2. Vault содержит секреты ВМ (хотя бы базовые)
3. DNS-запись существует и резолвится с других хостов в LAN
4. Jenkins-пайплайн для проверки успешно верифицировал ВМ
5. Prometheus Node Exporter установлен и работает, а метрики видны в Grafana.

?????: ????? ?? ?? ??????????

Как и в больших системах, полное удаление информации из КТС запрещено. Эта информация может понадобится позже. Вместо этого информация о хосте помечается как удаленная, за исключением пары моментов.

Чтобы вывести ВМ из эксплуатации нужно обратить изменения, а именно:

1. Удалить ВМ из списка мониторинга (изменить конфигурацию Prometheus);
2. Удалить саму ВМ в PVE и **более не занимать ее ID и имя хоста**;
3. Удалить DNS-записи, которые указывают на этот хост (на домен-контроллере);
4. Изменить информацию в NetBox по ВМ:
   - Изменить метку ВМ в NetBox: Active => Decommissioning (позже, после вывода - в Offline), а Start on boot перевести в Off;
   - Убрать с ВМ все теги, кроме информационных.
5. Удалить секреты из HashiCorp Vault, которые принадлежат этой ВМ;
6. Пометить ВМ в таблице КТС как удаленную (по аналогии с уже имеющимися записями);
7. Пометить ВМ на **схеме** как удаленную (по аналогии с уже имеющимися записями) или убрать ее вовсе.

> ВМ считается выведенной из эксплуатации только если все вышеописанные условия выполнены.

Revision #9
Created 2026-06-27 20:57:37 UTC by root
Updated 2026-06-28 01:27:39 UTC by root