

Резервное копирование и восстановление

Данный раздел содержит статьи полезные для настройки резервного копирования и восстановления в Nova Container Platform.

1. Резервное копирование и восстановление в Nova Container Platform

Резервное копирование и восстановление - это процессы создания резервной копии компонентов платформы Nova и последующего восстановления данных компонентов из этой копии, если что-то пойдет не так.

1.1. Поддерживаемые операции с мастер-узлами

Иногда может возникать необходимость остановить или перезапустить кластер Nova Container Platform для обслуживания оборудования или среды виртуализации. Вы можете воспользоваться соответствующими руководствами по корректному выключению и перезапуску кластера.

Перед выключением или перезапуском кластера вы должны сделать полную резервную копию мастер-узлов, которая включает в себя набор критически важных компонентов для работы платформы, таких как Etcd, StarVault, TLS-сертификаты, ключи шифрования, а также различные конфигурационные файлы.

i Кластерные TLS-сертификаты имеют срок действия 1 год с момента их выпуска при установке платформы. В течение этого периода вы можете рассчитывать на корректное включение или перезапуск кластера. Однако, если срок действия сертификатов истечет к моменту включения узлов кластера, вам будет необходимо обратиться к **поддержке платформы** для принудительного перевыпуска сертификатов.

Полная резервная копия мастер-узлов Kubernetes может быть выполнена как с помощью регулярного задания CronJob в Kubernetes, при котором данные сохраняются на предоставляемое пользователем NFS-хранилище, так и с помощью модуля Data Protection, в случае которого данные сохраняются во внешнем объектном хранилище.

1.2. Сценарии восстановления данных

Возможны ситуации, когда компоненты Nova Container Platform или кластер Kubernetes частично или полностью перестает функционировать из-за непредвиденных обстоятельств, например:

- При выходе из строя узлов виртуализации, повреждении оборудования или его компонентов, программных сбоев или потери сетевой связанности.
- При удалении критически важных данных на мастер-узлах платформы или в кластере Kubernetes.
- При потере кворума на мастер-узлах в кластерах Etcd, StarVault.

В разделе [Восстановление данных на мастер-узлах](#) вы можете найти подробную информацию о том, как действовать в том или ином сценарии.

1.3. Резервное копирование и восстановление пользовательских данных

Для резервного копирования и восстановления приложений (пользовательских данных) в Nova Container Platform используется дополнительный модуль Nova Data Protection на базе открытого ПО [Velero](#).

Velero поддерживает резервное копирование и восстановление пользовательских ресурсов Kubernetes на уровне пространств имен, а с помощью решения [Kopia](#) позволяет также осуществлять резервное копирование файловой системы, используемой приложениями и сервисами.

1.3.1. Основные требования

Для настройки и использования модуля Data Protection вам необходимо иметь учетную запись в кластере Kubernetes с правами администратора, а также доступ к какому-либо S3-совместимому объектному хранилищу, например:

- Объектное хранилище [K2 Cloud](#)
- Объектное хранилище [Yandex Cloud](#)
- Частные решения на базе [MinIO](#) и [Ceph](#)

Для подробной информации ознакомьтесь с разделом [Защита пользовательских данных с помощью модуля Data Protection](#)

1.3.2. Системные требования

Общие требования по вычислительным ресурсам можно найти [в статье](#)

2. Содержание раздела

- Резервное копирование мастер-узлов
- Восстановление данных на мастер-узлах
- Защита пользовательских данных с помощью модуля Data Protection



Веб-консоль

Веб-консоль Nova Container Platform это один из основных инструментов работы наравне с `kubectl`.

Она предоставляет возможность работы с kubernetes инженеру, который ранее не работал с данной технологией.

1. Содержание раздела

- [ConsoleLinks](#)
- [ConsoleYAMLSample](#)