WHITE PAPER

НАСТРОЙКА ИНТЕГРАЦИИ ПО «КИБЕР БЭКАП» И TATLIN.OBJECT

О WHITE PAPER

Данный документ описывает архитектурные принципы и подходы, а также рекомендации по их применению при построении корпоративных решений на основе продуктов производства компании YADRO.

Документ предназначен для широкой аудитории, но также может включать материалы, требующие специальной профессиональной подготовки, ориентированные на системных архитекторов, администраторов, сервисных инженеров и других ИТ-специалистов, участвующих в планировании, проектировании и внедрении комплексных решений.

! Представленная информация основана на результатах исследований, а также экспертизе специалистов YADRO. Документ носит не предписывающий, а информационный характер, целью которого является информирование получателей документа о предмете произведенного исследования и о его результатах. При этом конкретные результаты и эффективность конечных решений зависят от множества факторов, которые могут различаться в зависимости от особенностей инфраструктуры и условий эксплуатации. Ни при каких обстоятельствах YADRO не несет ответственность за последствия применения получателем документа рекомендаций, инструкций, подходов и решений, указанных в документе.

Запрещается копировать, воспроизводить, изменять, публиковать, передавать, распространять, продавать информацию (часть информации), содержащуюся в документе, или создавать производные работы на основе содержания документа без предварительного письменного разрешения YADRO.

Любая информация или утверждения относительно возможностей, емкости, производительности или других характеристик продукции, указанной в документе, предоставляются исключительно на условиях «как есть» и приведена исключительно в целях описания произведенного исследования. YADRO оставляет за собой право вносить изменения/обновлять информация в документе без уведомления.

«YADRO» является зарегистрированным товарным знаком ООО «КНС ГРУПП». Другие названия продуктов и компаний, упомянутые здесь, могут быть товарными знаками или торговыми наименованиями их соответствующих владельцев.

Актуальные версии документации публикуются на информационном ресурсе YADRO по адресу service.yadro.com.

ОГЛАВЛЕНИЕ

1. ОБ ЭКСПЕРТАХ 4
2. ВВЕДЕНИЕ 5
3. СОСТАВ ТЕСТОВОГО СТЕНДА 5
4. НАСТРОЙКА СЕРВЕРА «КИБЕР ИНФРАСТРУКТУРА 6.5.2» ДЛЯ ПОДКЛЮЧЕНИЯ К СХД TATLIN.OBJECT 6
   - 4.1. WebUI 6
   - 4.2. CLI 12
5. МЕТОДИКА ТЕСТИРОВАНИЯ 13
6. РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ 13
7. ВЫВОДЫ 13

ОБ ЭКСПЕРТАХ

Антон Морозов — ведущий ИТ-инженер и системный архитектор с более чем 15-летним опытом проектирования и внедрения высоконагруженных отказоустойчивых решений.

Начинал карьеру с глубокого погружения в Windows-экосистемы, что позволило сформировать уникальную экспертизу в построении сложных гибридных инфраструктур. В рамках сотрудничества с Microsoft и Ericsson реализовывал масштабные проекты по развертыванию IPTV-платформ для международных телеком-операторов (Vodafone Greece, TDC Denmark, Oi Brazil), где особое внимание уделял аспектам высокой доступности и бесперебойной миграции сервисов.

Сейчас в YADRO занимает позицию ведущего специалиста отдела объектных систем хранения данных, где фокусируется на:

- Оптимизации интеграции Tatlin Object Storage со сторонним ПО.
- Внедрении best practices по работе с распределенными системами хранения.

ВВЕДЕНИЕ

Данный документ описывает настройку интеграции ПО резервного копирования «Кибер Бэкап» и объектной системы хранения данных TATLIN.OBJECT.

Описана методика и дана оценка результатов исследования производительности резервного копирования виртуальных машин с использованием ПО «Кибер Бэкап» на СХД TATLIN.OBJECT.

	ВЕРСИИ ИСПОЛЬЗУЕМОГО ПО
TATLIN.OBJECT	1.7
Кибер Бэкап на базе ОС Ubuntu	18
Кибер Инфраструктура	6.5.2

СОСТАВ ТЕСТОВОГО СТЕНДА

> ! Все серверные и клиентские платформы были развернуты как виртуальные машины с использованием гипервизора VMware ESXi 8.0 U2.

1. Сервер «Кибер Бэкап 17.3» на базе ОС Ubuntu.
2. Сервер «Кибер Инфраструктура 6.5.2».

> !
> - Сервер развернут из официального ISO-образа.
> - Сервер выполняет роль шлюза для доступа сервера «Кибер Бэкап» к объектному хранилищу по протоколу S3.

3. VA-агент «Кибер Бэкап» для ESXi.
4. DNS-сервер на базе ОС Ubuntu с установленным DNS-сервером BIND

> ! Взаимодействие между узлами осуществляется по сети, для адресации используются FQDN-имена узлов. Для нормального функционирования системы требуется корректно работающая служба DNS. Необходимо заранее подготовить A-записи для сервера «Кибер Бэкап» и интерфейса управления сервера-шлюза «Кибер Инфраструктура».

5. Виртуальная машина на ОС Windows с установленным агентом «Кибер Бэкап».
6. Виртуальная машина на ОС Ubuntu с установленным агентом «Кибер Бэкап».
7. Система хранения данных TATLIN.OBJECT с установленной прошивкой версии 1.7.0.

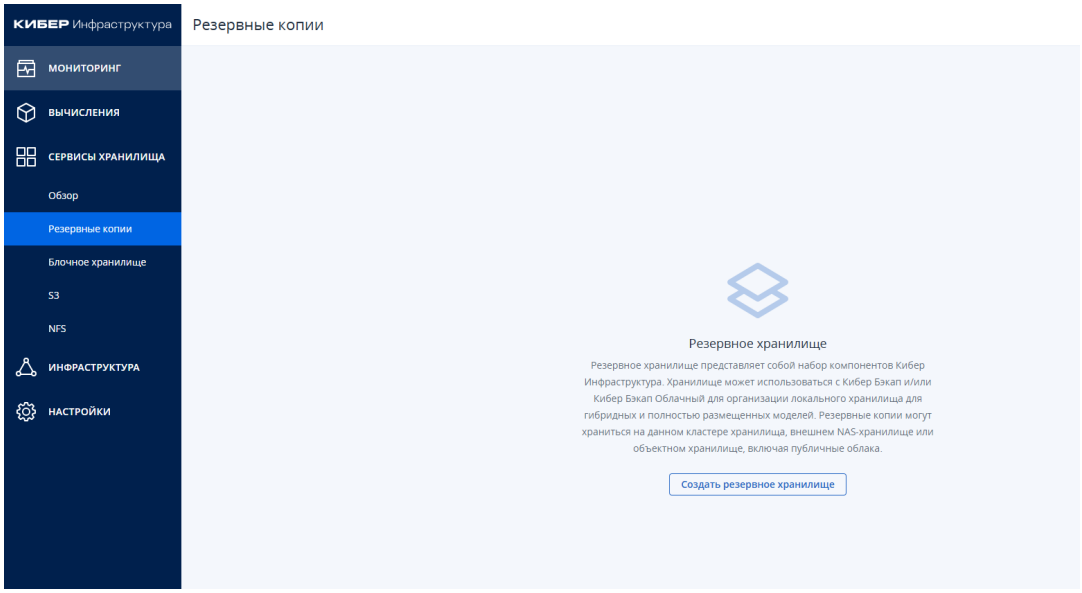
НАСТРОЙКА СЕРВЕРА «КИБЕР ИНФРАСТРУКТУРА 6.5.2» ДЛЯ ПОДКЛЮЧЕНИЯ К СХД TATLIN.OBJECT

В версии 6.5.2 подключение к TATLIN.OBJECT может быть настроено, как с помощью WebUI, так и с помощью CLI. Все настройки мы будем производить на установленном и настроенном сервере Кибер Инфраструктура 6.5.2, на котором уже развернут кластер.

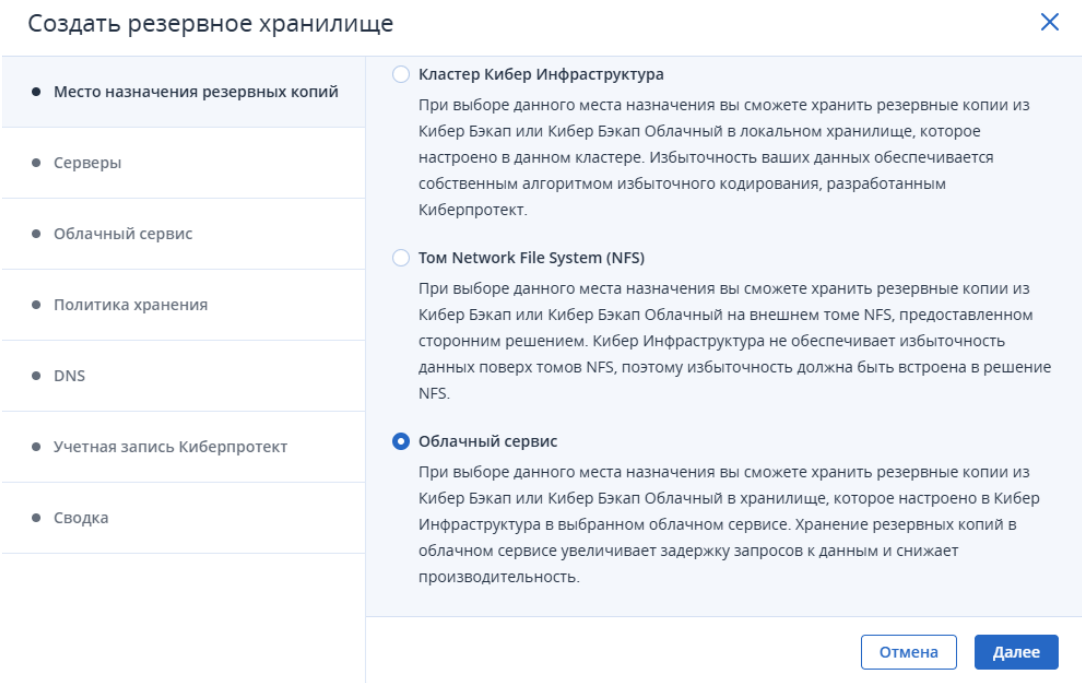
Для сервера Кибер Инфраструктура и управляющего сервера Кибер Бэкап созданы А-записи в днс сервере.

WebUI

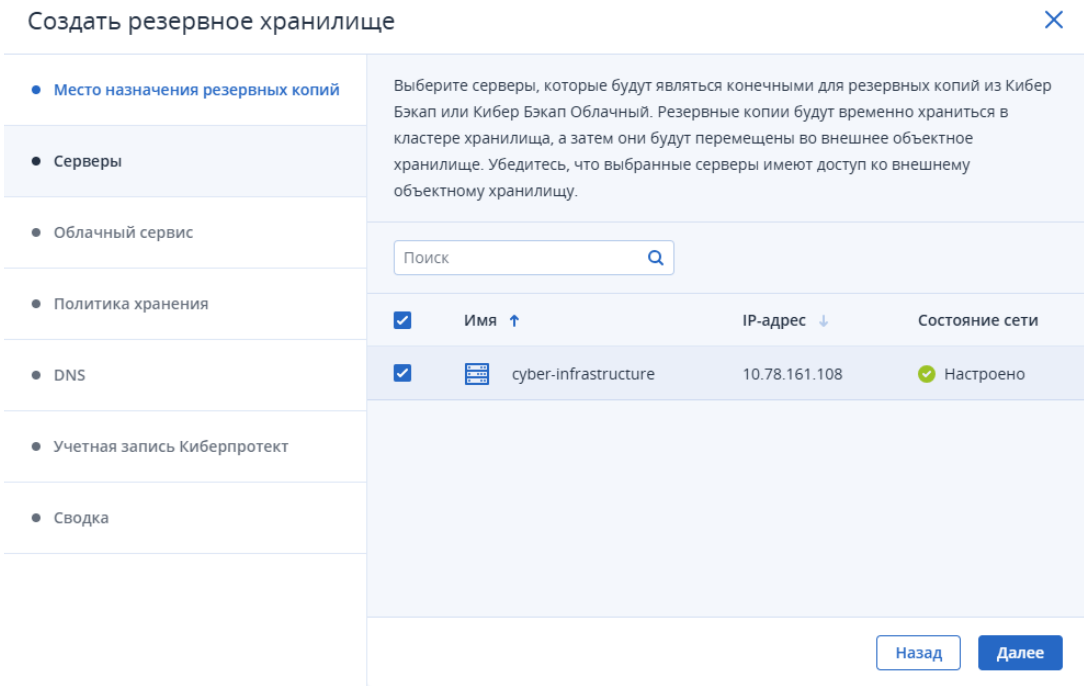
1. Перейдем в веб-интерфейс сервера Кибер Инфраструктура, раздел **Сервисы хранилища**, подраздел **Резервные копии**
2. Нажмем **Создать резервное хранилище**



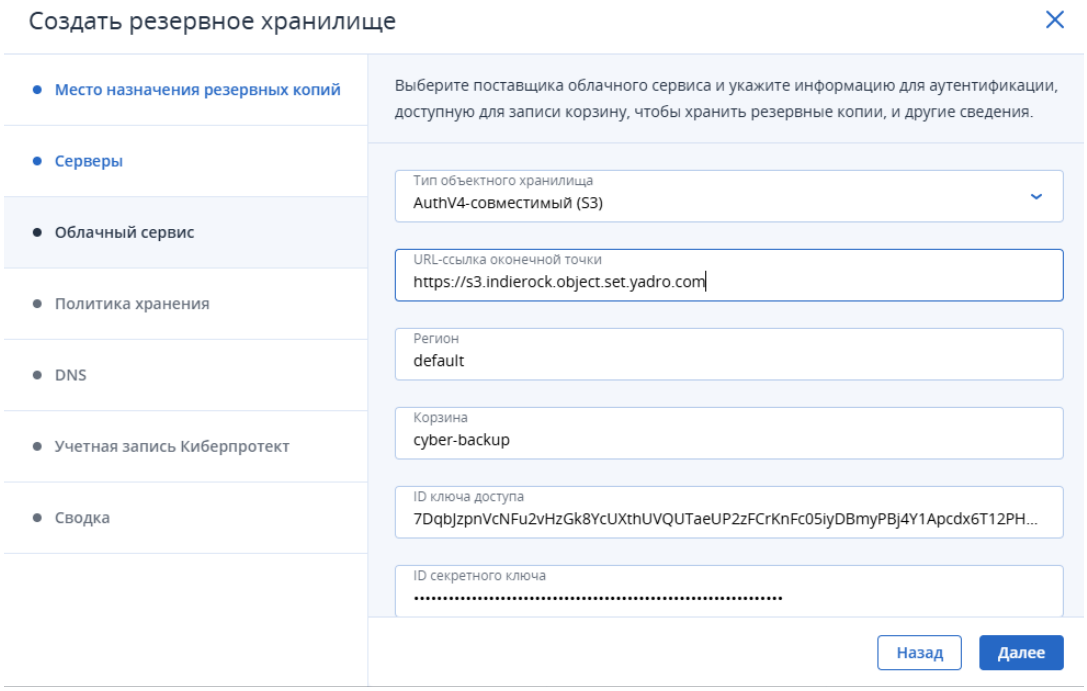
3. В появившемся диалоговом окне, выберем **Облачный сервис** и нажмем **Далее**.



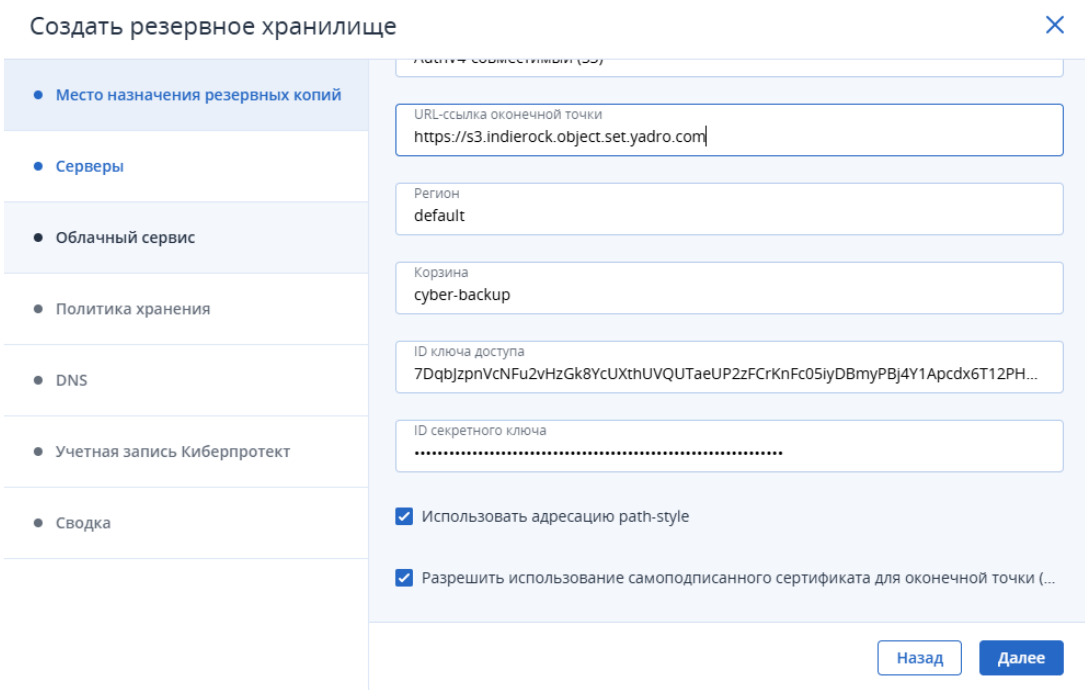
4. Выберем нужный нам сервер Кибер Инфраструктура, для которого мы хотим настроить хранилище и нажмем **Далее**.



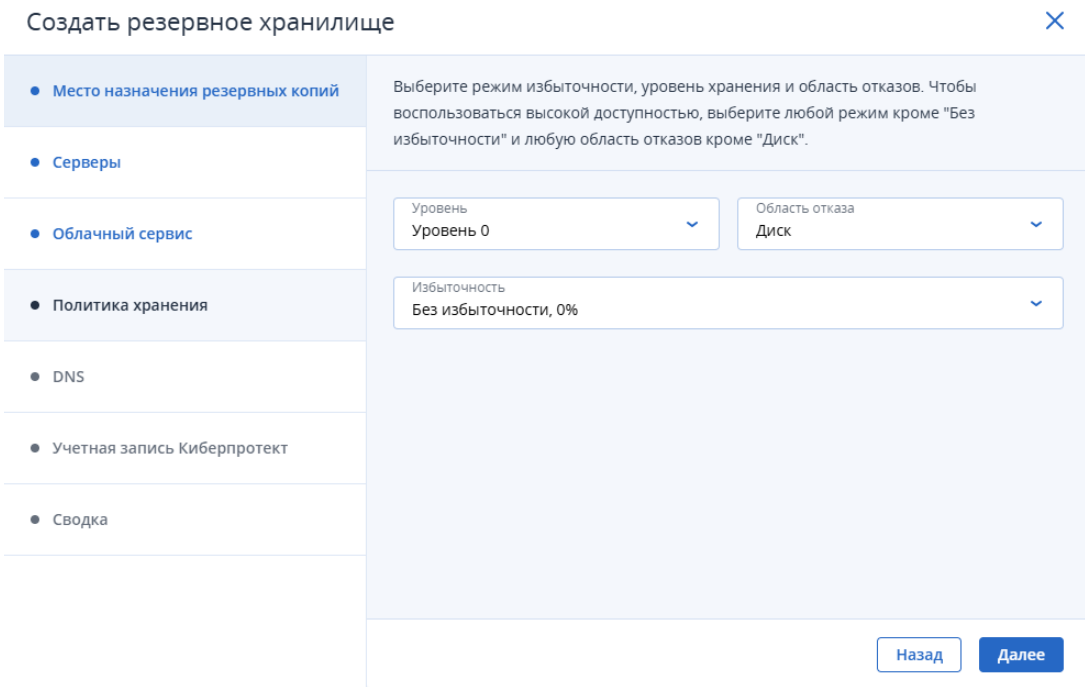
5. Выберем тип объетного хранилища **AuthV4-совместимый (S3)** и заполним все поля.



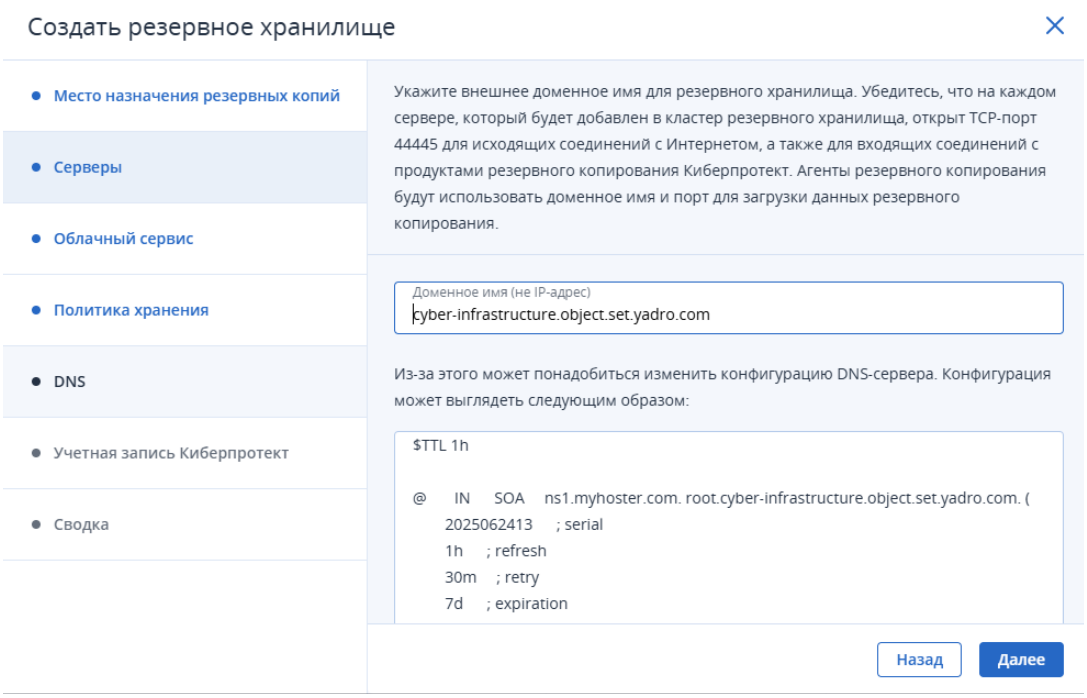
6. Также необходимо поставить галочку **Использовать адресацию path-style**.



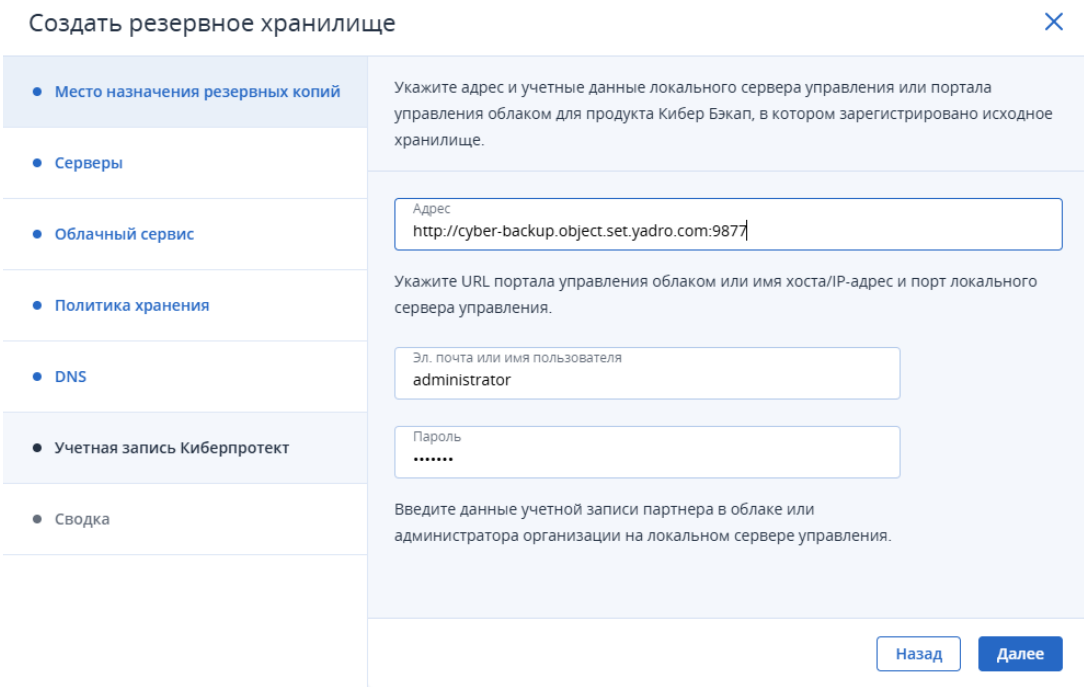
7. Зададим режим избыточности.



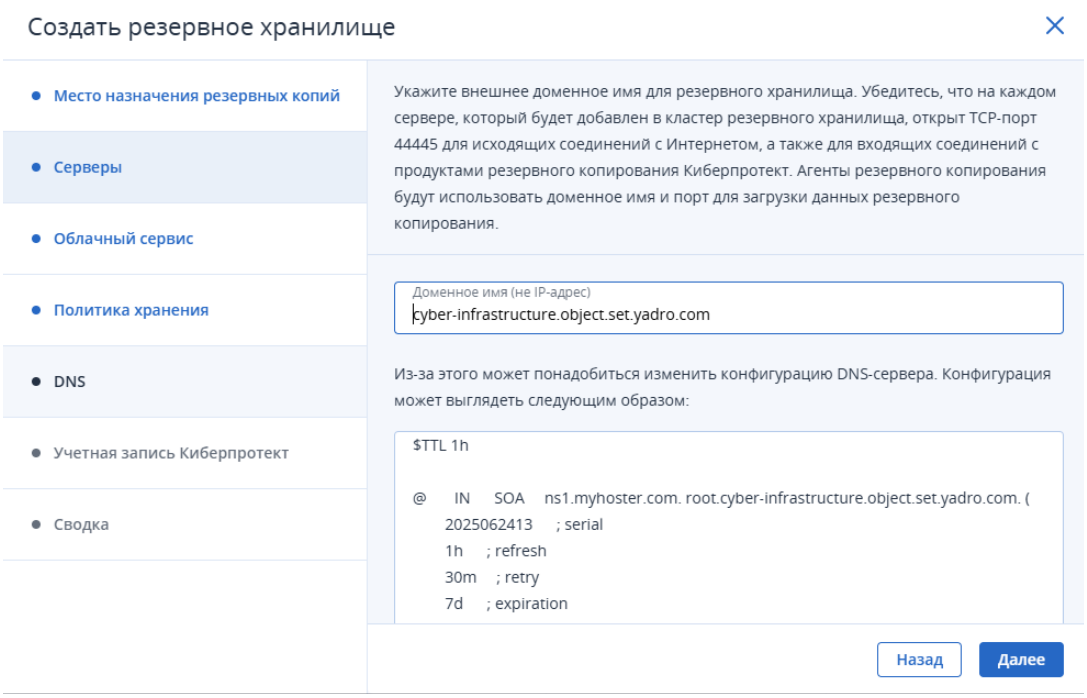
8. Укажем FQDN-имя для сервера Кибер Инфраструктура.



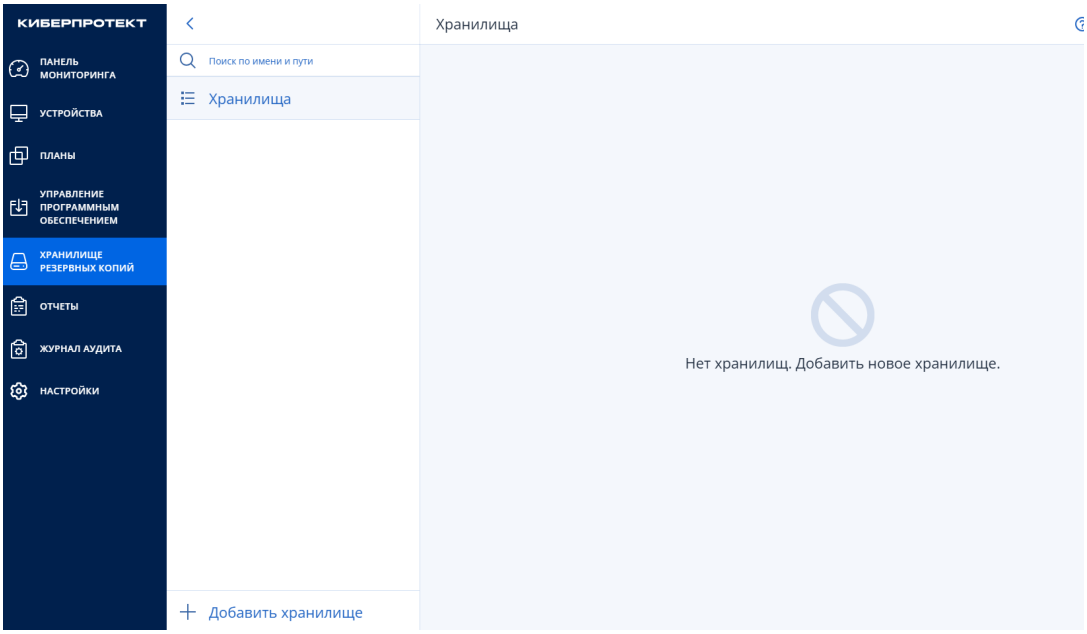
9. Укажем данные управляющего сервера Кибер Бэкап



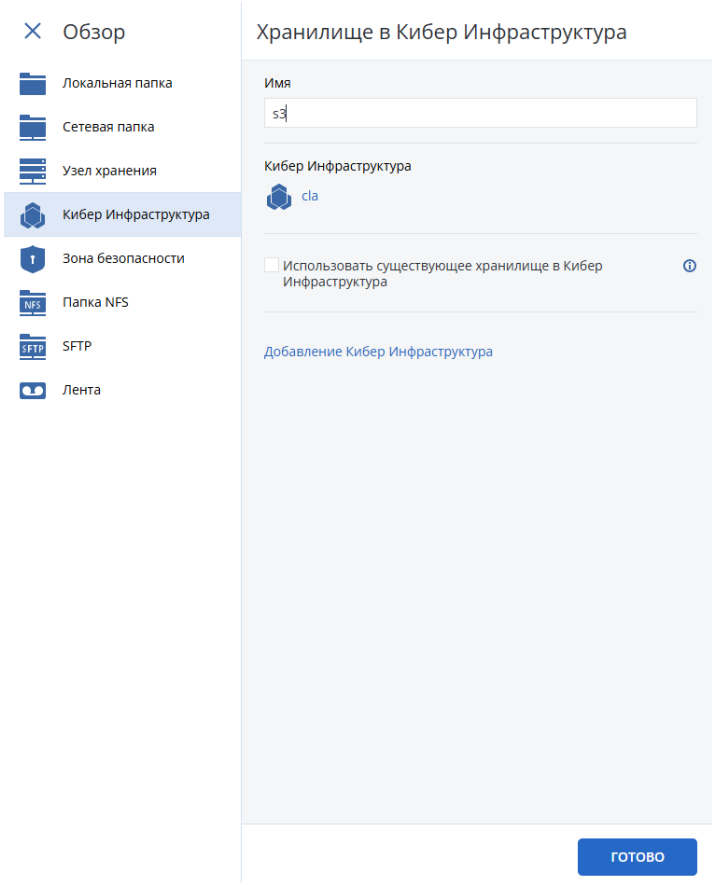
10. Завершим настройку, нажав кнопку **Создать**.



11. Перейдем в веб-интерфейс управляющего сервера Кибер Бэкап, в раздел **Хранилище резервных копий** и нажмем **Добавить хранилище**.



12. Выберем **Кибер Инфраструктура** и зададим имя нашему хранилищу, нажмем кнопку **Готово**.



Наше s3 хранилище готово к использованию в бэкап планах.

CLI

Для этого зайдите в консоль сервера Кибер Инфраструктура под учетной записью администратора и выполните следующие команды:

1. Получите NODE_ID с помощью команды:

```
vinfra node list
```

Запишите полученный `NODE_ID`. Эта информация потребуется для последующих шагов.

2. Экспортируйте пароль пользователя `root`:

```
export BACKUP_REG_PASSWORD='PASSWORD'
```

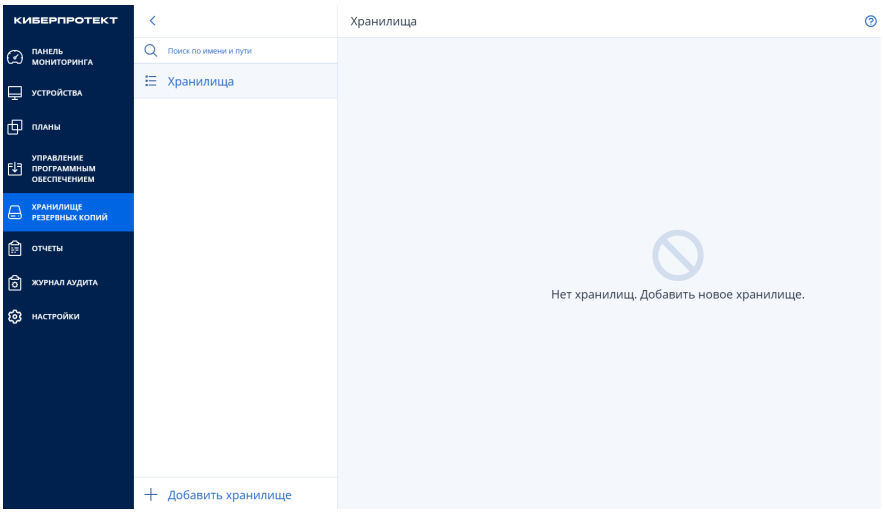
КОМАНДА	ОПИСАНИЕ КОМАНДЫ
PASSWORD	Пароль пользователя **root** на сервере «Кибер Бэкап».

3. Создайте кластер с помощью команды:

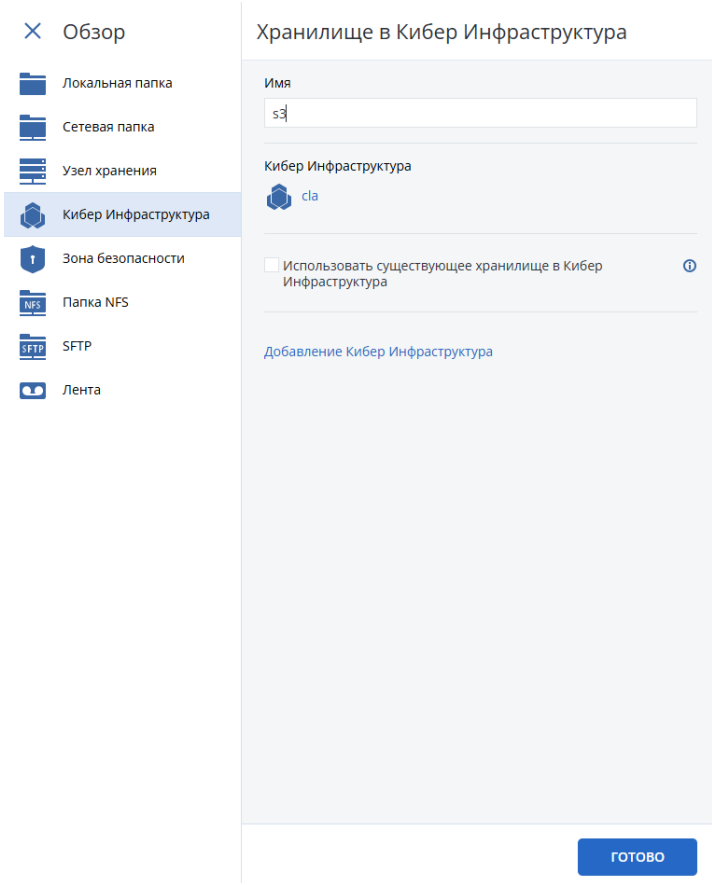
```
vinfra service backup cluster create --storage-type s3 --domain <SERVER_DOMAIN_NAME> --tier 0
--encoding 1+0 --failure-domain 1 --s3-flavor authv4 --s3-bucket <BUCKET_NAME> --s3-endpoint
<ENDPOINT_URL> --s3-access-key-id <ACCESS_KEY> --s3-secret-key-id <SECRET_KEY> --s3-cert-
verify false --reg-account root --reg-server <IP_OR_URL> --wait --nodes <NODE_ID>
```

КОМАНДА	ОПИСАНИЕ КОМАНДЫ
<SERVER_DOMAIN_NAME>	Доменное имя сервера «Кибер Инфраструктура».
<BUCKET_NAME>	Имя контейнера (бакета).
<ENDPOINT_URL>	Адрес подключаемого узла хранения в формате https://<endpoint_URL>.
<IP_OR_URL>	IP-адрес или URL сервера «Кибер Бэкап» в формате https://<URL:9877>.
<ACCESS_KEY>	Идентификатор ключа доступа по протоколу S3.
<SECRET_KEY>	Ключ доступа по протоколу S3.
<NODE_ID>	Данные из вывода команды vinfra node list.

4. Перейдем в веб-интерфейс управляющего сервера Кибер Бэкап, в раздел **Хранилище резервных копий** и нажмем **Добавить хранилище**.



5. Выберем Кибер Инфраструктура и зададим имя нашему хранилищу,нажмем кнопку **Готово**.



6. Наше s3 хранилище готово к использованию в бэкап планах.

МЕТОДИКА ТЕСТИРОВАНИЯ

Была проделана серия тестов:

1. Резервное копирование отдельной виртуальной машины с ОС Windows с помощью агента, установленного в ОС.
2. Резервное копирование отдельной виртуальной машины с ОС Linux с помощью агента, установленного в ОС.
3. Резервное копирование отдельной виртуальной машины с ОС Windows с помощью ESXi-агента.
4. Резервное копирование отдельной виртуальной машины с ОС Linux с помощью ESXi-агента.

РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ

В ходе проведения исследований была подтверждена функциональная совместимость ПО Кибер-Бэкап и Кибер-Инфраструктура с объектной системой хранения данных TATLIN.OBJECT.

ВЫВОДЫ

Объектная система хранения данных TATLIN.OBJECT может быть успешно использована в качестве хранилища резервных копий для решений на основе ПО Кибер Бэкап и Кибер Инфраструктура.