Резервное копирование мастер-узлов

Регулярное резервное копирование мастер-узлов Nova Container Platform необходимо, чтобы восстановить кластер в критических ситуациях. Рекомендуется организовать хранение резервных копий в инфраструктуре за пределами кластера Kubernetes. Резервное копирование не должно выполняться в пиковые часы нагрузки, поскольку процессы подготовки резервных копий оказывают влияние на дисковую подсистему мастер-узлов.

1. Объекты резервного копирования

Критически важными компонентами платформы, мастер-узлов и среды Kubernetes являются следующие сервисы:

- **Etcd**: основное хранилище данных, содержит всю информацию о ресурсах в Kubernetes.
- **StarVault**: основное хранилище TLS-сертификатов, секретов, учетных записей.

Кроме этого, в Nova Container Platform поддерживается опциональная возможность резервного копирования следующих объектов:

- **Токены StarVault (Unseal Tokens)**: токены для распечатывания (расшифровки) хранилища StarVault.
- **TLS-сертификаты**: сертификаты компонентов Kubernetes Control Plane и Nova Configuration Manager.
- **Ключи шифрования Etcd**: ключи, необходимые для шифрования секретов в Etcd.

2. Совместимость резервных копий

В Nova Container Platform поддерживается полное восстановление резервной копии только для патч-версии платформы (`x.y.Z`), в которой данная резервная копия создавалась.

Восстановление образов хранилищ Etcd и StarVault в несовместимые версии Nova Container Platform может привести к непредсказуемому поведению служебных сервисов платформы.

3. Выбор решения для резервного копирования

В Nova Container Platform поддерживается два основных решения для резервного копирования мастер-узлов:

- Регулярное задание *CronJob* в Kubernetes.
- С помощью дополнительного модуля Nova Data Protection и ПО Velero, входящего в его состав.

В каждом из решений запускается сервис Nova Backup Daemon, который выполняет резервное копирование информации на мастер-узлах. В зависимости от используемого решения в пользовательской инфраструктуре должно быть подготовлено соответствующее хранилище:

- В регулярном задании *CronJob* сервис Nova Backup Daemon использует том, куда выполняется сохранение резервной копии. Рекомендуется использовать в качестве тома подключаемое NFS-хранилище.
- При использовании ПО Velero из модуля Nova Data Protection в пользовательской инфраструктуре должно быть подготовлено и доступно S3-совместимое объектное хранилище. В данном сценарии сервис Nova Backup Daemon сохраняет резервную копию мастер-узлов локально, а затем выполняется резервная копия сервиса с его данными с помощью Velero.

Вы можете использовать наиболее подходящее решение в зависимости от вашей инфраструктуры и доступных ресурсов.

В разделе Резервное копирование и восстановление пользовательских данных вы можете ознакомиться с требованиями для установки модуля Nova Data Protection.

4. Настройка резервного копирования мастер-узлов

В данном разделе описана процедура настройки резервного копирования мастер-узлов платформы Nova Container Platform:

- используя возможности запуска регулярных заданий CronJob в Kubernetes;
- с помощью ПО Velero, входящего в состав модуля Data Protection.

4.1. Настройка резервного копирования с помощью регулярного задания CronJob

Необходимые условия

- ✓ У вас есть доступ к кластеру с учетной записью, имеющей роль `cluster-admin` в Kubernetes.
- ✓ Вы установили утилиту `kubectl` для работы с Kubernetes.
- ✓ У вас подготовлено NFS-хранилище для резервных копий.

Порядок действий:

1. Подготовьте манифест кастомизации (*Kustomization*) в зависимости от количества мастер-узлов в кластере Kubernetes:

   ▸ **3 мастер-узла**

   ▸ **1 мастер-узел**

2. Установите параметры резервного копирования.

   Укажите переменные окружения сервиса Nova Backup Daemon:

Параметр	Значение по умолчанию	Описание
`INCLUDE_STARVAULT_UNSEAL_TOKENS`	`true`	Добавление в архив резервной копии токенов для распечатывания StarVault.
`INCLUDE_PKI_DATA`	`true`	Добавление в архив резервной копии всех выпущенных TLS-сертификатов для платформы.
`INCLUDE_DATA_ENCRYPTION_CONFIG`	`true`	Добавление в архив резервной копии ключей шифрования Etcd.
`INCLUDE_STARVAULT_DB_BACKUP`	`true`	Добавление в архив резервной копии снимка БД StarVault.
`RETENTION_PERIOD_DAYS`	`7`	Количество дней, в течение которых необходимо хранить резервные копии на внешнем хранилище.

   Информация

   Для каждого мастер-узла создается собственная резервная копия выбранных данных с учетом следующей информации:

   - Резервная копия Etcd создается всегда и только однократно на одном из мастер-узлов платформы.
   - Для получения полного набора токенов для распечатывания StarVault необходимо иметь резервные копии всех мастер-узлов.

- Резервное копирование TLS-сертификатов не включает приватные ключи центров сертификации платформы, поскольку они не являются эскпортируемыми и хранятся только в БД StarVault.
- Управление количеством дней хранения резервных копий доступно только для решения резервного копирования с помощью регулярного задания CronJob. При использовании модуля Nova Data Protection политика хранения данных определяется средствами ПО Velero.

Укажите спецификацию тома `backup-volume`, предназначенного для хранения резервных копий.

Например, для NFS-хранилища используйте спецификацию:

```yaml
spec:
  volumes:
  - name: backup-volume
    nfs:
      server: nfs-share.nova.internal
      path: /nova-cluster-8b4e9344-9dcd-4c64-b98a-4a8a08a53da6
      readOnly: false
```

где `nfs.server` - DNS-имя вашего NFS-сервера или его IP-адрес, `nfs.path` - путь для хранения резервных копий.

Укажите график резервного копирования в формате Cron, например, для выполнения резервных копий каждый день в 4:00:

```yaml
schedule: "0 4 * * *"
```

3. Сохраните полученный манифест и установите его в кластер Kubernetes с помощью Nova Console или *kubectl*.

   Пример

   ```bash
   kubectl apply -f nova-release-cluster-backup-cronjob.yaml

   kustomization.kustomize.toolkit.fluxcd.io/nova-release-cluster-backup-
   cronjob created
   ```

4. Проверьте статус кастомизации:

   ```bash
   kubectl get ks nova-release-cluster-backup-cronjob -n nova-gitops
   ```

   Пример

```
kubectl get ks nova-release-cluster-backup-cronjob -n nova-gitops

NAME                                  AGE   READY   STATUS
nova-release-cluster-backup-cronjob   41s   True    Applied revision:
v5.1.2@sha1:6789a4025a1edd244044677ed43d8087018e5a7d
```

5. Получите информацию об установленном регулярном задании Cronjob:

```
kubectl get cronjobs.batch -n nova-cluster-backup
```

Пример

```
kubectl get cronjobs.batch -n nova-cluster-backup

NAME                    SCHEDULE    SUSPEND   ACTIVE   LAST SCHEDULE   AGE
nova-backup-scheduled   0 4 * * *   False     1        7s              14m
```

Регулярное задание запустится автоматически в указанное в графике время.

В процессе работы задания на мастер-узлах будут запускаться сервисы Nova Backup Daemon, а по завершению работы их статус можно будет отследить в пространстве имен `nova-cluster-backup`. Статус может быть *Completed* в успешном случае, и *Error* в случае ошибки.

Для просмотра статуса резервного копирования выполните команду:

```
kubectl get pods -n nova-cluster-backup
```

Пример

```
kubectl get pods -n nova-cluster-backup

NAME                                    READY   STATUS      RESTARTS   AGE
nova-backup-scheduled-28629407-0-v7qbv   0/1     Completed   0          24s
nova-backup-scheduled-28629407-1-t2wbt   0/1     Completed   0          24s
nova-backup-scheduled-28629407-2-h6hq9   0/1     Completed   0          24s
```

4.1.1. Проверка резервных копий на внешнем хранилище

Вы также можете проверить наличие резервных копий на внешнем хранилище. На примере ниже показана директория внешнего NFS-сервера, куда выполняется резервное копирование мастер-узлов кластера Nova Container Platform.

Пример

```bash
ls -la /storage/nova-364f9cbe-b209-4f3a-a4d4-9fe36a81afef/

drwxr-xr-x. 2 nobody nobody     4096 Jun  7 15:47 .
drwxr-xr-x. 3 nobody nobody       55 Jun  7 14:44 ..
-rw-r--r--. 1 root   root   16209258 Jun  7 15:47 etcd_snapshot_nova-v5.1.2_k8s-v1.27.11_2024-06-07_124701.db.tar.gz
-rw-------. 1 root   root     219326 Jun  7 15:47 nova-master-1-nova-internal_kuberesources_2024-06-07_124701.tar.gz
-rw-------. 1 root   root     219247 Jun  7 15:47 nova-master-2-nova-internal_kuberesources_2024-06-07_124701.tar.gz
-rw-------. 1 root   root     219279 Jun  7 15:47 nova-master-3-nova-internal_kuberesources_2024-06-07_124700.tar.gz
-rw-------. 1 root   root     314521 Jun  7 15:47 starvault_snapshot_nova-v5.1.2_2024-06-07_124701.db
```

Для архивов резервных копий применяется следующая схема именования:

- Имя архива резервной копии Etcd имеет формат `etcd_snapshot_nova-<Версия Nova>_k8s-<Версия Kubernetes>_<Время создания копии>.db.tar.gz`.
- Имена архивов резервных копий конфигураций мастер-узлов имеют формат `<Имя узла в Kubernetes>_kuberesources_<Время создания копии>.tar.gz`.
- Имя архива резервной копии StarVault имеет формат `starvault_snapshot_nova-<Версия Nova>_<Время создания копии>1.db`.

4.2. Настройка резервного копирования с помощью Velero

Необходимые условия

- ✓ У вас есть доступ к кластеру с учетной записью, имеющей роль `cluster-admin` в Kubernetes.
- ✓ Вы установили утилиту `kubectl` для работы с Kubernetes.
- ✓ Вы установили модуль Data Protection в Nova Container Platform.
- ✓ Вы настроили утилиту velero для работы с резервными копиями Velero.
- ✓ Вы подготовили внешнее хранилище Velero `BackupStorageLocation`.

1. Для установка сервиса Nova Backup Daemon с помощью модуля Data Protection в Nova Container Platform используйте представленный далее манифест кастомизации.

```yaml
apiVersion: kustomize.toolkit.fluxcd.io/v1
kind: Kustomization
metadata:
  name: nova-release-cluster-backup-rbac
  namespace: nova-gitops
```

```yaml
  labels:
    nova-application-group: data-protection
    kustomization.nova-platform.io/cluster: "true"
spec:
  serviceAccountName: kustomize-controller
  commonMetadata:
    labels:
      app.kubernetes.io/managed-by: Nova
  interval: 10m
  retryInterval: 30s
  timeout: 5m
  prune: false
  force: true
  sourceRef:
    kind: GitRepository
    name: nova-release-gitrepo-main
  path: ./resources/cluster-backup-rbac
---
apiVersion: kustomize.toolkit.fluxcd.io/v1
kind: Kustomization
metadata:
  name: nova-release-cluster-backup-velero
  namespace: nova-gitops
  labels:
    nova-application-group: data-protection
    kustomization.nova-platform.io/cluster: "true"
spec:
  serviceAccountName: kustomize-controller
  commonMetadata:
    labels:
      app.kubernetes.io/managed-by: Nova
  interval: 10m
  retryInterval: 30s
  timeout: 5m
  prune: false
  force: true
  dependsOn:
  - name: nova-release-velero-main
  - name: nova-release-cluster-backup-rbac
  sourceRef:
    kind: GitRepository
    name: nova-release-gitrepo-main
  path: ./resources/cluster-backup-velero
  postBuild:
    substituteFrom:
    - kind: ConfigMap
      name: nova-gitops-common-substitute-config
  healthChecks:
    - apiVersion: apps/v1
      kind: DaemonSet
```

```
      name: nova-backup-daemon
      namespace: nova-cluster-backup
```

2. Проверьте статус кастомизации:

```
BASH
kubectl get ks nova-release-cluster-backup-velero -n nova-gitops
```

Пример

```
BASH
kubectl get ks nova-release-cluster-backup-velero -n nova-gitops

NAME                                AGE   READY   STATUS
nova-release-cluster-backup-velero   39s   True    Applied revision:
v5.1.2@sha1:86f53cb7e4dbacb29fa42f2c1c9814fa6aec7a07
```

3. Получите информацию об установленном сервисе Nova Backup Daemon:

```
BASH
kubectl get ds nova-backup-daemon -n nova-cluster-backup
```

Пример

```
BASH
kubectl get ds nova-backup-daemon -n nova-cluster-backup

NAME                 DESIRED   CURRENT   READY   UP-TO-DATE   AVAILABLE
NODE SELECTOR                            AGE
nova-backup-daemon   3         3         3       3            3
node-role.kubernetes.io/control-plane=   103s
```

4. Подготовьте и установите манифест плана резервного копирования мастер-узлов в кластер Kubernetes с помощью Nova Console или *kubectl*.

```
YAML
apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: control-plane-backup
  namespace: nova-cluster-backup
spec:
  paused: false
  schedule: 0 4 * * *
  template:
    csiSnapshotTimeout: 0s
    includedNamespaces:
    - nova-cluster-backup
    includedResources:
    - 'daemonsets'
    - 'pods'
    labelSelector:
      matchLabels:
```

```
        app.kubernetes.io/component: nova-backup-daemon
    metadata: {}
    ttl: 24h0m0s
```

Укажите график резервного копирования в формате Cron, например, для выполнения резервных копий каждый день в 4:00:

YAML

```yaml
schedule: "0 4 * * *"
```

Пример

BASH

```
kubectl create -f backup-schedule.yaml

schedule.velero.io/control-plane-backup created
```

5. Проверьте статус плана резервного копирования:

   ▸ **kubectl**

   ▸ **Velero CLI**

6. Дождитесь выполнения резервного копирования и проверьте статус плана резервного копирования:

   ▸ **kubectl**

   ▸ **Velero CLI**

7. Проверьте статус отдельных заданий резервного копирования:

   ▸ **kubectl**

   ▸ **Velero CLI**

4.2.1. Проверка резервных копий на внешнем хранилище

Вы также можете проверить наличие резервных копий в объектном хранилище. На примере ниже показан пример резервных копий в объектном хранилище, куда выполняется резервное копирование мастер-узлов кластера Nova Container Platform.

Вы можете использовать любой совместимый с вашим объектным хранилищем консольный клиент или веб-интерфейс.

Пример

```
BASH
aws s3 ls s3://velero-backup-bucket --endpoint-url https://s3.nova.internal

                           PRE backups/
                           PRE kopia/
```

В директории `backups/` находятся резервные копии спецификаций ресурсов (манифестов) Kubernetes.

Пример

```
BASH
aws s3 ls s3://velero-backup-bucket/backups/ --endpoint-url
https://s3.nova.internal

                           PRE control-plane-backup-20240610121525/
                           PRE control-plane-backup-20240610131525/
                           PRE control-plane-backup-20240610141525/
                           PRE control-plane-backup-20240610151525/
```

В директории `kopia/` находятся резервные копии файлов сервиса Nova Backup Daemon: резервные копии Etcd, StarVault, PKI и др.

Пример

```
BASH
aws s3 ls s3://velero-backup-bucket/kopia/nova-cluster-backup/ --endpoint-url
https://s3.nova.internal

2024-06-10 15:15:43        747
_log_20240610121542_f5ce_1718021742_1718021743_1_6bd1da03b924c1be6ec634227e336f1
9
2024-06-10 15:15:45       1685
_log_20240610121544_c120_1718021744_1718021745_1_dfc7e059b0394a85ca25fe7ecce7ab2
9
2024-06-10 15:16:04       1755
_log_20240610121603_6ea6_1718021763_1718021764_1_64d9d4b3f4b3d8c4eb7dc310be213d1
a
2024-06-10 15:16:28       2640
_log_20240610121626_aa10_1718021786_1718021788_1_0eeb3acc062071d4a84bd08f8ab8262
1
2024-06-10 16:15:32       1919
_log_20240610131531_287a_1718025331_1718025332_1_60750784af3ee83ed569fbe2e82d40e
e
2024-06-10 16:15:39       1941
_log_20240610131537_04d8_1718025337_1718025339_1_564e1ea03aade8ccfb2236efc04f1fb
```

```
7
2024-06-10 16:15:50       2737
_log_20240610131548_7f66_1718025348_1718025350_1_5595519176d088bf2512ae9d2251381
6
2024-06-10 16:16:26       3775
_log_20240610131625_6f8c_1718025385_1718025386_1_c60f0d81f4b09128277702e43ddf365
5
2024-06-10 17:15:32       2097
_log_20240610141530_363a_1718028930_1718028932_1_dd21e1a8aa835344b058b311aa58ad7
8
2024-06-10 17:15:39       3334
_log_20240610141537_b56d_1718028937_1718028939_1_efd4f6b0da8be6a04d392e7aa4e8e20
b
2024-06-10 17:15:51       2875
_log_20240610141549_8d12_1718028949_1718028951_1_75f3ceb8dce9a244c56bd08631a3476
1
2024-06-10 17:16:26       1320
_log_20240610141625_ca81_1718028985_1718028986_1_c4975114b6b94de09792c2bbe869406
1
2024-06-10 18:15:32       2261
_log_20240610151531_7b9a_1718032531_1718032532_1_7325bf67c58d582df1363ddaff938cf
a
2024-06-10 18:15:39       2392
_log_20240610151537_074c_1718032537_1718032539_1_4c8b33484e2ee5c7cc21d411b7eeefb
d
2024-06-10 18:15:50       3330
_log_20240610151548_2718_1718032548_1718032550_1_5b2cb4f36c3124cc78acf28574555b6
5
2024-06-10 18:16:26       1825
_log_20240610151625_aff3_1718032585_1718032586_1_9be5f2ab4206fd4b43b49fdc8dfde30
3
2024-06-10 15:15:42         30 kopia.blobcfg
2024-06-10 18:16:26        620 kopia.maintenance
2024-06-10 15:15:42       1075 kopia.repository
2024-06-10 18:15:31   26726736 p0941d6b0f97eccef7587b5cbff2207f6-
s77d051db729eba1e129
...
```

Защита пользовательских данных с помощью модуля Data Protection

В данном разделе описана защита пользовательских данных с помощью модуля Data Protection.

1. Установка модуля Nova Data Protection

Для установки модуля Data Protection в Nova Container Platform с настройками по умолчанию используйте представленный далее манифест кастомизации.

▸ Манифест кастомизации

1.1. Установка в Kubernetes

Необходимые условия

- ✓ У вас есть доступ к кластеру с учетной записью, имеющей роль `cluster-admin` в Kubernetes.
- ✓ Вы установили утилиту `kubectl` для работы с Kubernetes.

Порядок действий

1. Сохраните полученный манифест и установите его в кластер Kubernetes с помощью Nova Console или *kubectl*.

   Пример

   ```
   BASH
   kubectl apply -f nova-release-cluster-backup-velero.yaml

   kustomization.kustomize.toolkit.fluxcd.io/nova-release-velero-main created
   ```

2. Проверьте статус кастомизации:

   ```
   BASH
   kubectl get ks nova-release-velero-main -n nova-gitops
   ```

   Пример

   ```
   BASH
   kubectl get ks nova-release-velero-main -n nova-gitops
   ```

```
NAME                          AGE   READY   STATUS
nova-release-velero-main      55s   True    Applied revision:
v5.1.2@sha1:86f53cb7e4dbacb29fa42f2c1c9814fa6aec7a07
```

3. Проверьте состояние запущенных компонентов Velero, выполнив команду:

```bash
kubectl get pods -n nova-cluster-backup
```

Пример

```bash
kubectl get pods -n nova-cluster-backup

NAME                            READY   STATUS    RESTARTS   AGE
velero-7877767f4-zkdbh          1/1     Running   0          22s
node-agent-b4wrh                1/1     Running   0          22s
node-agent-hpcj5                1/1     Running   0          22s
node-agent-tmvvp                1/1     Running   0          22s
node-agent-vhh6b                1/1     Running   0          22s
node-agent-w2qbb                1/1     Running   0          22s
node-agent-xk5l4                1/1     Running   0          22s
node-agent-xlh6k                1/1     Running   0          22s
```

На данном этапе установка модуля с настройками по умолчанию завершена, и вы можете перейти к его настройке.

2. Настройка хранилища резервных копий

В модуле Data Protection ПО Velero поставляется с плагином для подключения к объектному хранилищу, совместимому с Amazon Web Services (AWS) S3. Вы также можете использовать любые S3-совместимые хранилища для подключения к Velero.

Для подключения объектного хранилища в Velero вам необходимо настроить в Kubernetes объект *Secret*, в котором должны быть установлены учетные данные. Как правило, это переменные `aws_access_key_id` и `aws_secret_access_key`. Кроме этого, вам потребуется переопределить точку подключения к объектному хранилищу.

Следуйте инструкциям ниже, чтобы настроить хранилище резервных копий.

2.1. Настройка секрета доступа к объектному хранилищу

Секрет доступа к объектному хранилищу должен быть размещен в среде Kubernetes. Для корректной работы Velero должен быть создан секрет по умолчанию, который будет использоваться для доступа к объектному хранилищу в случаях, когда отдельный секрет явно не указан.

При дальнейшей настройке вы можете создать любое дополнительное количество секретов.

Размещение секрета доступа к объектному хранилищу в StarVault не дает явных преимуществ в безопасности платформы. При этом значительно повышается сложность эксплуатации решения по резервному копированию, особенно, когда резервное копирование выполняется в разные бакеты или хранилища, где требуются отдельные учетные записи.

Необходимые условия

- ✓ У вас есть доступ к кластеру с учетной записью, имеющей роль `cluster-admin` в Kubernetes.
- ✓ У вас подготовлена учетная запись для доступа к объектному хранилищу.

Порядок действий:

1. Создайте на локальной машине файл, например, `cloud-credentials`. В данном файле необходимо указать учетную запись по умолчанию для подключения к объектному хранилищу.

   Пример

   ```
   BASH
   cat << EOF > ./cloud-credentials
   [default]
   aws_access_key_id=<AWS_ACCESS_KEY_ID>
   aws_secret_access_key=<AWS_SECRET_ACCESS_KEY>
   EOF
   ```

2. Создайте секрет по умолчанию:

   ```
   BASH
   kubectl create secret generic cloud-credentials -n nova-cluster-backup --
   from-file cloud=cloud-credentials
   ```

   Пример

   ```
   BASH
   kubectl create secret generic cloud-credentials -n nova-cluster-backup --
   from-file cloud=cloud-credentials

   secret/cloud-credentials created
   ```

2.2. Настройка ключа шифрования данных

Резервные копии персистентных данных (файлов) зашифровываются с помощью ключа, хранимого в StarVault. Данный ключ уникален для каждой инсталляции Nova Container Platform. При необходимости, вы можете сменить ключ шифрования следуя процедуре ниже.

Рекомендуется сменить ключ шифрования до настройки каких-либо планов резервного копирования. После настройки ключа шифрования вам необходимо выполнить перезапуск Velero с помощью команды:

```bash
kubectl -n nova-cluster-backup rollout restart deployment/velero
```

Необходимые условия

- ✓ У вас есть доступ к кластеру с учетной записью, имеющей роль `cluster-admin` в Kubernetes.
- ✓ У вас есть токен доступа к хранилищу секретов StarVault с привилегиями `root`.
- ✓ У вас подготовлена учетная запись для доступа к объектному хранилищу.

Порядок действий

1. Подключитесь к StarVault следуя процедуре, описанной в разделе Подключение к StarVault.
2. Перейдите в раздел **Secrets**, выберете секрет `nova-secrets`.
3. В секрете `nova-secrets` перейдите в `credentials`, далее в `nova-velero`.
4. Создайте новую версию секрета, используя кнопку “*Create new version*” измените значение ключа `repository_password` на новое.

2.3. Настройка BackupStorageLocation

Для регистрации объектного хранилища в Velero вам необходимо создать CR *BackupStorageLocation*.

Порядок действий

1. Подготовьте манифест CR *BackupStorageLocation* и установите его в кластер Kubernetes с помощью Nova Console или *kubectl*.

```yaml
apiVersion: velero.io/v1
kind: BackupStorageLocation
metadata:
  labels:
    app.kubernetes.io/managed-by: Nova
  name: default ①
  namespace: nova-cluster-backup ②
spec:
  config:
    region: ru-dc-1 ③
    s3Url: https://s3.nova.internal ④
  default: true ⑤
  objectStorage:
```

```
    bucket: velero-backup-bucket ⑥
  provider: aws ⑦
  credential:
    name: cloud-credentials ⑧
    key: cloud
```

① Имя CR *BackupStorageLocation*.

② Пространство имен, где регистрируется объектное хранилище.

③ (Опционально) регион для подключения к объектному хранилищу.

④ Точка подключения к объектному хранилищу.

⑤ Установить объектное хранилище по умолчанию.

⑥ Имя бакета для хранения резервных копий.

⑦ Имя провайдера для подключения к объектному хранилищу.

⑧ Имя секрета доступа к объектному хранилищу.

Пример

BASH

```
kubectl create -f backup-storage-location.yaml

backupstoragelocation.velero.io/default created
```

2. Проверьте статус регистрации объектного хранилища:

▸ **kubectl**

▸ **Velero CLI**

На данном этапе настройка хранилища резервных копий завершена, и вы можете перейти к настройкам планов резервного копирования.

3. Восстановление резервных копий мастер-узлов

Перед тем, как восстанавливать какой-либо компонент мастер-узла или кластера Kubernetes в Nova Container Platform с помощью резервной копии Velero, необходимо сперва восстановить копию сервиса Nova Backup Daemon, в котором хранится резервная копия мастер-узлов. Кроме этого, поддерживается сценарий восстановления данных из объектного хранилища без доступа к Velero с помощью Kopia.

В разделах ниже описаны обе процедуры восстановления данных.

3.1. Восстановление данных с помощью Velero

При восстановлении данных с помощью Velero в кластер Kubernetes восстанавливается копия сервиса Nova Backup Daemon, в которой находятся резервные копии мастер-узлов. Вы можете перенести данные копии на локальную машину и перейти к восстановлению отдельных компонентов мастер-узлов и среды Kubernetes.

Необходимые условия

- ✓ У вас есть доступ к кластеру с учетной записью, имеющей роль `cluster-admin` в Kubernetes.
- ✓ Вы установили утилиту `kubectl` для работы с Kubernetes.
- ✓ Вы настроили утилиту velero для работы с резервными копиями Velero.

Порядок действий

1. Получите список резервных копий и выберете копию для восстановления:

   ▸ **kubectl**

   ▸ **Velero CLI**

2. Восстановите выбранную резервную копию в кластер Kubernetes:

   ```
   BASH
   velero restore create <RESTORE_NAME> \
       --from-backup <BACKUP_NAME> \
       --namespace-mappings nova-cluster-backup:nova-cluster-restore
   ```

   Для восстановления резервной копии используйте следующие данные:

   - `RESTORE_NAME` - имя задания на восстановление резервной копии
   - `BACKUP_NAME` - имя выбранной резервной копии

   ⛔ Не изменяйте значение ключа `--namespace-mappings` при создании задания на восстановление резервной копии. Копия восстанавливается в пространство имен `nova-cluster-restore`, сохраняя работоспособность сервиса Nova Backup Daemon в пространстве имен `nova-cluster-backup`.

   Пример

   ```
   BASH
   velero restore create restore-control-plane-backup-20240610161525 \
       --from-backup control-plane-backup-20240610161525 \
       --namespace-mappings nova-cluster-backup:nova-cluster-restore

   Restore request "restore-control-plane-backup-20240610161525" submitted
   successfully.
   Run `velero restore describe restore-control-plane-backup-
   ```

```
20240610161525` or `velero restore logs restore-control-plane-backup-
20240610161525` for more details.
```

3. Проверьте статус задания на восстановление резервной копии:

```
BASH
velero restore get restore-control-plane-backup-20240610161525
```

Пример

```
BASH
velero restore get restore-control-plane-backup-20240610161525

NAME                                              BACKUP
STATUS      STARTED                            COMPLETED
ERRORS   WARNINGS   CREATED                            SELECTOR
restore-control-plane-backup-20240610161525   control-plane-backup-
20240610161525   Completed   2024-06-11 15:33:51 +0000 UTC   2024-06-11
15:33:57 +0000 UTC   0        3          2024-06-11 15:33:51 +0000 UTC
<none>
```

4. Получите список Pod'ов сервиса Nova Backup Daemon в пространстве имен `nova-cluster-restore`:

```
BASH
kubectl get pods -n nova-cluster-restore
```

Пример

```
BASH
kubectl get pods -n nova-cluster-restore

NAME                       READY   STATUS    RESTARTS   AGE
nova-backup-daemon-2xf9p   1/1     Running   0          78s
nova-backup-daemon-s5zws   1/1     Running   0          78s
nova-backup-daemon-z4lmn   1/1     Running   0          77s
```

5. Скопируйте резервные копии мастер-узлов с каждого из Pod:

```
BASH
PODNAME=<POD_NAME>; \
    for file in $(kubectl exec $PODNAME -n nova-cluster-restore -c backup-
daemon -- ls /opt/backup); \
    do kubectl cp -c backup-daemon nova-cluster-
restore/$PODNAME:/opt/backup/$file $PWD/$file; done
```

В качестве `<POD_NAME>` укажите имя Pod сервиса Nova Backup Daemon.

Пример

```
BASH
PODNAME=nova-backup-daemon-2xf9p; \
    for file in $(kubectl exec $PODNAME -n nova-cluster-restore -c backup-
```

```
daemon -- ls /opt/backup); \
    do kubectl cp -c backup-daemon nova-cluster-
restore/$PODNAME:/opt/backup/$file $PWD/$file; done
```

Файлы резервной копии будут сохранены в текущую директорию на локальной машине пользователя.

6. Проверьте список полученных файлов:

   Пример

```
ls -la

drwxr-xr-x. 2 root root     4096 Jun 11 19:09 .
drwxr-xr-x. 7 root root     4096 Jun 11 18:39 ..
-rw-r--r--. 1 root root 68989925 Jun 11 19:09 etcd_snapshot_nova-v5.1.2_k8s-
v1.27.11_2024-06-11_050616.db.tar.gz
-rw-r--r--. 1 root root 33970260 Jun 11 19:09 nova-master-1-nova-
internal_kuberesources_2024-06-11_050616.tar.gz
-rw-r--r--. 1 root root 33971757 Jun 11 19:08 nova-master-2-nova-
internal_kuberesources_2024-06-11_050535.tar.gz
-rw-r--r--. 1 root root 33973476 Jun 11 19:08 nova-master-3-nova-
internal_kuberesources_2024-06-11_050556.tar.gz
-rw-r--r--. 1 root root   375225 Jun 11 19:09 starvault_snapshot_nova-
v5.1.2_2024-06-11_050616.db
```

7. После восстановления резервной копии сервиса Nova Backup Daemon удалите задание на восстановление:

```
velero restore delete <RESTORE_NAME>
```

   В качестве `<RESTORE_NAME>` укажите имя задания на восстановление резервной копии, которое необходимо удалить.

   Пример

```
velero restore delete restore-control-plane-backup-20240610161525

Are you sure you want to continue (Y/N)? y
Request to delete restore "restore-control-plane-backup-20240610161525"
submitted successfully.
The restore will be fully deleted after all associated data (restore files
in object storage) are removed.
```

   Также удалите восстановленный сервис Nova Backup Daemon:

   Пример

```bash
kubectl delete ds -n nova-cluster-restore nova-backup-daemon
```

3.2. Восстановление данных с помощью Kopia

Для восстановления данных из объектного хранилища напрямую без участия Velero вам необходимо будет подключиться к репозиторию резервных копий *Kopia* с помощью утилиты *Kopia CLI*. Данный репозиторий инициализируется с помощью Velero автоматически в процессе настройки резервного копирования. Вы сможете получить файлы, которые были подготовлены сервисом Nova Backup Daemon. Имея данные файлы, вы сможете перейти к восстановлению отдельных компонентов мастер-узлов и среды Kubernetes.

Необходимые условия

- ✓ Вы установили утилиту Kopia CLI.
- ✓ У вас есть ключ шифрования резервных копий.
- ✓ У вас есть доступ к бакету в объектном хранилище, где сохранены резервные копии.

Порядок действий

1. Подключитесь к хранилищу резервных копий с помощью Kopia CLI:

   ```bash
   kopia repository connect s3 \
       --access-key=<AWS_ACCESS_KEY_ID> \
       --secret-access-key=<AWS_SECRET_ACCESS_KEY> \
       --bucket=<BUCKET_NAME> \
       --prefix=kopia/nova-cluster-backup/ \
       --endpoint=<S3_ENDPOINT_URL>

   Enter password to open repository:
   <ENCRYPTION_PASSWORD>
   ```

   Для подключения используйте следующие данные:

   - `AWS_ACCESS_KEY_ID` и `AWS_SECRET_ACCESS_KEY` - учетные данные для подключения к объектному хранилищу
   - `BUCKET_NAME` - имя бакета для хранения резервных копий.
   - `S3_ENDPOINT_URL` - точка подключения к объектному хранилищу без указания протокола.

     Пример

     ```bash
     kopia repository connect s3 \
         --access-key="ASIAIOSFODNN7EXAMPLE" \
         --secret-access-key="wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY" \
         --bucket=velero-backup-bucket \
     ```

```
    --prefix=kopia/nova-cluster-backup/ \
    --endpoint=s3.nova.internal

Enter password to open repository: ********

Connected to repository.
```

2. Получите список идентификаторов снапшотов в хранилище резервных копий:

```bash
kopia snapshot list --all -l
```

Пример

```bash
kopia snapshot list —all -l

default@default:/host_pods/1eeb2ac9-36de-4a9c-a1d1-
a0ac4618f6fd/volumes/kubernetes.io~empty-dir/backup-volume 2024-06-11
12:15:40 MSK k702d957ec030e814fbc61bcd63d2d316 34 MB drwxrwxrwx files:1
dirs:1 (latest-3,hourly-3) pins:velero-pin 2024-06-11 13:15:40 MSK
kf576cc276650d10920e96b48d162ea5a 34 MB drwxrwxrwx files:1 dirs:1 (latest-
2,hourly-2) pins:velero-pin 2024-06-11 14:15:40 MSK
k2d67a575200c57344846b221c36e9bd6 34 MB drwxrwxrwx files:1 dirs:1 (latest-
1,hourly-1,daily-1,weekly-1,monthly-1,annual-1) pins:velero-pin

default@default:/host_pods/4f4aaa17-da1a-4c30-a587-
535604a991b1/volumes/kubernetes.io~empty-dir/backup-volume 2024-06-11
12:15:57 MSK kfcafeadd427239980e47f4eceeed244a 94.2 MB drwxrwxrwx files:3
dirs:1 (latest-3,hourly-3) pins:velero-pin 2024-06-11 13:15:58 MSK
k31d18913f2a147722f292609b987ad15 93.3 MB drwxrwxrwx files:3 dirs:1 (latest-
2,hourly-2) pins:velero-pin 2024-06-11 14:15:58 MSK
k570cf06adf55dbf2e87b2959f148c3b2 92.3 MB drwxrwxrwx files:3 dirs:1 (latest-
1,hourly-1,daily-1,weekly-1,monthly-1,annual-1) pins:velero-pin

default@default:/host_pods/fd076d09-d8f6-480e-addf-
03f3fa33f633/volumes/kubernetes.io~empty-dir/backup-volume 2024-06-11
12:15:47 MSK kf3872b5f18ef1fd536fe1d75cb2fa160 34 MB drwxrwxrwx files:1
dirs:1 (latest-3,hourly-3) pins:velero-pin 2024-06-11 13:15:47 MSK
k7113f38a1b63f03caf4ca1cb179550fb 34 MB drwxrwxrwx files:1 dirs:1 (latest-
2,hourly-2) pins:velero-pin 2024-06-11 14:15:47 MSK
kc950a4ee5808557fe2c3d01df22ff4e3 34 MB drwxrwxrwx files:1 dirs:1 (latest-
1,hourly-1,daily-1,weekly-1,monthly-1,annual-1) pins:velero-pin +
```

В выводе команды отображен список резервных копий томов `backup-volume` для трех разных Pod сервиса Nova Backup Daemon, имеющих UID:

- `1eeb2ac9-36de-4a9c-a1d1-a0ac4618f6fd`
- `4f4aaa17-da1a-4c30-a587-535604a991b1`
- `fd076d09-d8f6-480e-addf-03f3fa33f633`

Для того, чтобы проверить соответствие данных резервных копий узлам в Kubernetes, вы можете выполнить команду:

```
kubectl get pod -l app.kubernetes.io/component=nova-backup-daemon -n
nova-cluster-backup \
    -o custom-
columns=PodName:.metadata.name,UID:.metadata.uid,NODE:.spec.nodeName
```

Пример

```
kubectl get pod -l app.kubernetes.io/component=nova-backup-daemon -n
nova-cluster-backup \
    -o custom-
columns=PodName:.metadata.name,UID:.metadata.uid,NODE:.spec.nodeName

PodName                    UID                                    NODE
nova-backup-daemon-2xf9p   1eeb2ac9-36de-4a9c-a1d1-a0ac4618f6fd   nova-
master-2.nova.internal
nova-backup-daemon-s5zws   fd076d09-d8f6-480e-addf-03f3fa33f633   nova-
master-3.nova.internal
nova-backup-daemon-z4lmn   4f4aaa17-da1a-4c30-a587-535604a991b1   nova-
master-1.nova.internal
```

3. Восстановите необходимую резервную копию:

```
kopia snapshot restore <SNAPSHOT_ID>
```

В качестве `SNAPSHOT_ID` укажите тот идентификатор снапшота, временная метка которого соответствует требуемой точке восстановления.

Пример

```
kopia snapshot restore k570cf06adf55dbf2e87b2959f148c3b2

Restoring to local filesystem (/root/k570cf06adf55dbf2e87b2959f148c3b2) with
parallelism=8...
Processed 4 (92.3 MB) of 3 (92.3 MB) 69.9 MB/s (100.0%) remaining 0s.
Processed 4 (92.3 MB) of 3 (92.3 MB) 69.9 MB/s (100.0%) remaining 0s.
Restored 3 files, 1 directories and 0 symbolic links (92.3 MB).
```

4. Проверьте восстановленные данные:

Пример

```
ls -la /root/k570cf06adf55dbf2e87b2959f148c3b2/
итого 90160
drwxrwxrwx.  2 root root     4096 Jun 11 14:15 .
```

```
dr-xr-x---. 89 root root     4096 Jun 11 14:50 ..
-rw-r--r--.  1 root root 58044113 Jun 11 14:15 etcd_snapshot_nova-
v5.1.2_k8s-v1.27.11_2024-06-11_111549.db.tar.gz
-rw-------.  1 root root 33970429 Jun 11 14:15 nova-master-1-nova-
internal_kuberesources_2024-06-11_111549.tar.gz
-rw-------.  1 root root   292009 Jun 11 14:15 starvault_snapshot_nova-
v5.1.2_2024-06-11_111549.db
```

Для архивов резервных копий применяется следующая схема именования:

- Имя архива резервной копии Etcd имеет формат `etcd_snapshot_nova-<Версия Nova>_k8s-<Версия Kubernetes>_<Время создания копии>.db.tar.gz`.
- Имена архивов резервных копий конфигураций мастер-узлов имеют формат `<Имя узла в Kubernetes>_kuberesources_<Время создания копии>.tar.gz`.
- Имя архива резервной копии StarVault имеет формат `starvault_snapshot_nova-<Версия Nova>_<Время создания копии>1.db`.

> Резервная копия только одного из мастер-узлов включает копии Etcd и StarVault.

5. Повторите действия по восстановлению для оставшихся Pod’ов сервиса Nova Backup Daemon.
6. Отключитесь от хранилища резервных копий:

```bash
kopia repository disconnect
```

> В настоящее время в Velero используется общий статический ключ шифрования для всех создаваемых репозиториев резервного копирования. Это означает, что любой, кто имеет доступ к вашему хранилищу резервных копий, может расшифровать ваши резервные копии. Обязательно ограничьте доступ к хранилищу резервных копий соответствующим образом.