앱 보호

Astra Control Center

NetApp
March 12, 2024

목차

앱 보호

보호 개요

Astra Control Center를 사용하여 앱에 대한 백업, 클론, 스냅샷 및 보호 정책을 생성할 수 있습니다. 앱을 백업하면 서비스 및 관련 데이터를 가능한 한 사용할 수 있습니다. 재해 시나리오 중에 백업에서 복원하면 애플리케이션 및 관련 데이터를 중단 없이 완벽하게 복구할 수 있습니다. 백업, 클론, 스냅샷을 사용하면 랜섬웨어, 우발적인 데이터 손실 및 환경 재해와 같은 일반적인 위협으로부터 보호할 수 있습니다. "Astra Control Center에서 사용 가능한 데이터 보호 유형과 사용 시기에 대해 알아보십시오".

또한 재해 복구에 대비하여 애플리케이션을 원격 클러스터로 복제할 수 있습니다.

애플리케이션 보호 워크플로우

다음 예제 워크플로를 사용하여 앱 보호를 시작할 수 있습니다.

[1개] 모든 앱을 보호합니다

앱을 즉시 보호하려면 "모든 앱의 수동 백업을 생성합니다".

[2개] 각 앱에 대한 보호 정책을 구성합니다

향후 백업 및 스냅샷 자동화 "각 앱에 대한 보호 정책을 구성합니다". 예를 들어 주별 백업과 일별 스냅샷으로 시작할 수 있으며 두 가지 모두에 대해 한 달 동안 보존할 수 있습니다. 수동 백업 및 스냅샷보다 보호 정책을 사용하여 백업 및 스냅샷을 자동화하는 것이 좋습니다.

[세 가지] 보호 정책을 조정합니다

앱과 사용 패턴이 변경되면 최적의 보호 기능을 제공하기 위해 필요에 따라 보호 정책을 조정합니다.

[네] 앱을 원격 클러스터로 복제합니다

"애플리케이션 복제" NetApp SnapMirror 기술을 사용하여 원격 클러스터로 Astra Control은 스냅샷을 원격 클러스터에 복제하여 비동기식 재해 복구 기능을 제공합니다.

[다섯] 재해가 발생할 경우 최신 백업 또는 복제를 사용하여 원격 시스템으로 앱을 복구합니다

데이터 손실이 발생하면 를 통해 복구할 수 있습니다 "최신 백업을 복원하는 중입니다" 각 앱에 대해 먼저 그런 다음 최신 스냅샷을 복구할 수 있습니다(사용 가능한 경우). 또는 원격 시스템에 복제를 사용할 수 있습니다.

스냅샷 및 백업으로 애플리케이션 보호

자동화된 보호 정책을 사용하거나 필요에 따라 스냅샷 및 백업을 수행하여 모든 애플리케이션을 보호합니다. Astra Control Center UI 또는 를 사용할 수 있습니다 "Astra Control API" 앱을 보호합니다.

이 작업에 대해

- * 앱 배포 *: Helm을 사용하여 앱을 배포하는 경우 Astra Control Center에 Helm 버전 3이 필요합니다. Helm 3으로 배포된 애플리케이션 관리 및 복제(또는 Helm 2에서 Helm 3으로 업그레이드)가 완벽하게 지원됩니다. Helm 2와 함께 배포된 앱은 지원되지 않습니다.
- * (OpenShift 클러스터에만 해당) 정책 추가 *: OpenShift 클러스터에서 앱을 호스팅하기 위한 프로젝트를 생성할 때 프로젝트(또는 Kubernetes 네임스페이스)에 SecurityContext UID가 할당됩니다. Astra Control Center에서 앱을 보호하고 OpenShift의 다른 클러스터 또는 프로젝트로 앱을 이동하려면 해당 앱을 UID로 실행할 수 있는 정책을 추가해야 합니다. 예를 들어 다음 OpenShift CLI 명령은 WordPress 앱에 적절한 정책을 부여합니다.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

앱 데이터 보호와 관련된 다음 작업을 수행할 수 있습니다.

- 보호 정책을 구성합니다
- 스냅샷을 생성합니다
- 백업을 생성합니다
- ONTAP - NAS - 경제성 작업을 위한 백업 및 복원 지원
- 변경 불가능한 백업을 생성합니다
- 스냅샷 및 백업을 봅니다
- 스냅샷을 삭제합니다
- 백업을 취소합니다
- 백업을 삭제합니다

보호 정책을 구성합니다

보호 정책은 정의된 일정에 따라 스냅샷, 백업 또는 둘 다를 생성하여 앱을 보호합니다. 시간별, 일별, 주별 및 월별 스냅샷과 백업을 생성하도록 선택할 수 있으며, 보존할 복제본 수를 지정할 수 있습니다.

시간당 한 번 이상 백업 또는 스냅샷을 자주 실행해야 하는 경우 를 수행할 수 있습니다 "Astra Control REST API를 사용하여 스냅샷과 백업을 생성합니다".

WORM(Write Once Read Many) 버킷에 대한 변경 불가능한 백업을 생성하는 보호 정책을 정의하는 경우 백업의 보존 시간이 버킷에 대해 구성된 보존 기간보다 짧지 않은지 확인합니다.

백업 및 복제 일정을 오프셋하여 일정이 겹치지 않도록 합니다. 예를 들어, 매시간 맨 위에서 백업을 수행하고 5분 오프셋 및 10분 간격으로 복제를 시작하도록 예약합니다.

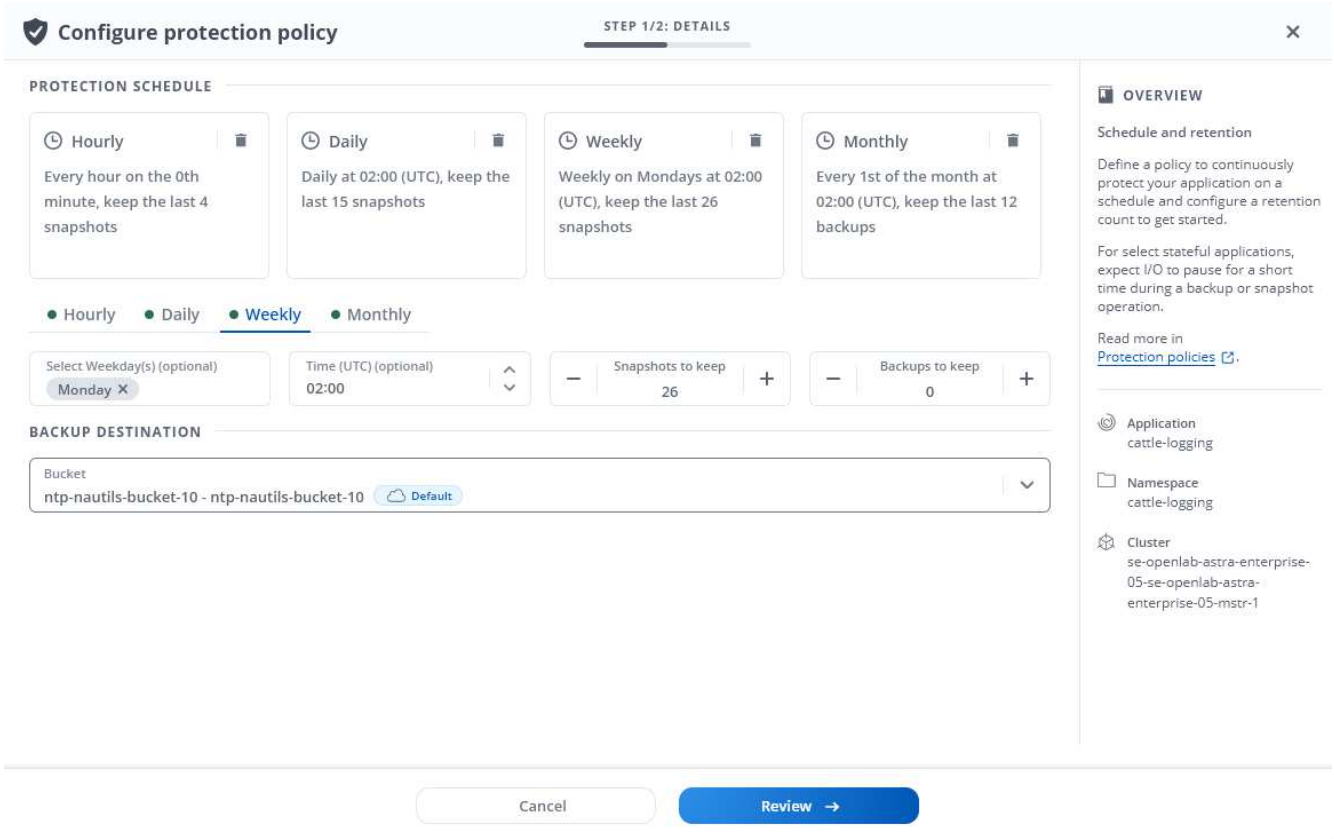
단계

1. 응용 프로그램 * 을 선택한 다음 앱 이름을 선택합니다.
2. 데이터 보호 * 를 선택합니다.
3. 보호 정책 구성 * 을 선택합니다.
4. 시간별, 일별, 주별 및 월별로 유지할 스냅샷 및 백업 수를 선택하여 보호 스케줄을 정의합니다.

시간별, 일별, 주별 및 월별 스케줄을 동시에 정의할 수 있습니다. 보존 레벨을 설정하기 전에는 스케줄이 활성화되지 않습니다.

백업의 보존 레벨을 설정할 때 백업을 저장할 버킷을 선택할 수 있습니다.

다음 예에서는 스냅샷 및 백업의 경우 매시간, 일별, 주별 및 월별로 4개의 보호 스케줄을 설정합니다.



5. Review * 를 선택합니다.
6. 보호 정책 설정 * 을 선택합니다

결과

Astra Control은 정의한 스케줄 및 보존 정책을 사용하여 스냅샷 및 백업을 생성하고 유지함으로써 데이터 보호 정책을 구현합니다.

스냅샷을 생성합니다

언제든지 주문형 스냅샷을 생성할 수 있습니다.

이 작업에 대해

Astra Control은 다음 드라이버를 통해 지원되는 스토리지 클래스를 사용하여 스냅샷 생성을 지원합니다.

- `ontap-nas`
- `ontap-san`
- `ontap-san-economy`

앱이 에서 지원하는 저장소 클래스를 사용하는 경우 `ontap-nas-economy` 드라이버, 스냅샷을 생성할 수 없습니다. 스냅샷에 대체 스토리지 클래스를 사용합니다.

단계

1. 응용 프로그램 * 을 선택합니다.
2. 원하는 앱의 * Actions * 열에 있는 옵션 메뉴에서 * Snapshot * 을 선택합니다.
3. 스냅샷 이름을 사용자 지정하고 * 다음 * 을 선택합니다.
4. 스냅샷 요약을 검토하고 * Snapshot * 을 선택합니다.

결과

스냅샷 프로세스가 시작됩니다. 데이터 보호 * > * 스냅샷 * 페이지의 * 상태 * 열에서 상태가 * 정상 * 인 경우 스냅샷이 성공합니다.

백업을 생성합니다

언제든지 앱을 백업할 수 있습니다.

이 작업에 대해

Astra Control의 버킷은 사용 가능한 용량을 보고하지 않습니다. Astra Control에서 관리되는 앱을 백업 또는 클론 복제하기 전에 적절한 스토리지 관리 시스템에서 버킷 정보를 확인하십시오.

앱이 에서 지원하는 저장소 클래스를 사용하는 경우 `ontap-nas-economy` 드라이버, 당신은 필요합니다 백업 및 복원을 활성화합니다 기능. 을(를) 정의했는지 확인합니다 `backendType` 매개 변수 을 선택합니다 "Kubernetes 스토리지 오브젝트입니다" 을 값으로 사용합니다 `ontap-nas-economy` 보호 작업을 수행하기 전에

Astra Control은 다음 드라이버를 통해 지원되는 스토리지 클래스를 사용하여 백업 생성을 지원합니다.

- `ontap-nas`
- `ontap-nas-economy`
- `ontap-san`
- `ontap-san-economy`

단계

1. 응용 프로그램 * 을 선택합니다.
2. 원하는 앱의 * Actions * 열에 있는 옵션 메뉴에서 * Back Up * 을 선택합니다.
3. 백업 이름을 사용자 지정합니다.
4. 기존 스냅샷에서 앱을 백업할지 여부를 선택합니다. 이 옵션을 선택하면 기존 스냅샷 목록에서 선택할 수 있습니다.
5. 스토리지 버킷 목록에서 백업할 대상 버킷을 선택합니다.
6. 다음 * 을 선택합니다.
7. 백업 요약을 검토하고 * 백업 * 을 선택합니다.

결과

Astra Control은 앱 백업을 생성합니다.

- 네트워크에 정전이 발생했거나 비정상적으로 느린 경우 백업 작업이 시간 초과될 수 있습니다. 이로 인해 백업이 실패합니다.
- 실행 중인 백업을 취소해야 하는 경우 의 지침을 따릅니다 백업을 취소합니다. 백업을 삭제하려면 백업이 완료될 때까지 기다린 다음 의 지침을 따르십시오 백업을 삭제합니다.
- 데이터 보호 작업(클론, 백업, 복원)과 후속 영구 볼륨 크기 조정 후 UI에 새 볼륨 크기가 표시되기까지 최대 20분이 지연됩니다. 데이터 보호 작업이 몇 분 내에 성공적으로 완료되며 스토리지 백엔드에 관리 소프트웨어를 사용하여 볼륨 크기 변경을 확인할 수 있습니다.

ONTAP - NAS - 경제성 작업을 위한 백업 및 복원 지원

Astra Control Provisioner는 를 사용하는 스토리지 백엔드에 대해 설정할 수 있는 백업 및 복원 기능을 제공합니다 `ontap-nas-economy` 스토리지 클래스.

시작하기 전에

- 있습니다 "Astra Control Provisioner를 활성화했습니다".
- Astra Control에서 애플리케이션을 정의했습니다. 이 응용 프로그램은 이 절차를 완료할 때까지 제한된 보호 기능을 제공합니다.
- 있습니다 `ontap-nas-economy` 스토리지 백엔드의 기본 스토리지 클래스로 선택됩니다.

구성 단계를 위해 확장합니다

1. ONTAP 스토리지 백엔드에서 다음을 수행합니다.

   a. 를 호스팅하는 SVM을 찾습니다 `ontap-nas-economy`응용 프로그램의 볼륨을 기반으로 합니다.

   b. 볼륨이 생성된 ONTAP에 연결된 터미널에 로그인합니다.

   c. SVM에 대한 스냅샷 디렉토리 숨기기:

   > 이러한 변경은 전체 SVM에 영향을 줍니다. 숨겨진 디렉토리에 계속 액세스할 수 있습니다.

   ```
   nfs modify -vserver <svm name> -v3-hide-snapshot enabled
   ```

   +

   > ONTAP 스토리지 백엔드의 스냅샷 디렉토리가 숨겨져 있는지 확인합니다. 이 디렉토리를 숨기지 않으면 특히 NFSv3을 사용하는 경우에는 애플리케이션에 대한 액세스가 손실될 수 있습니다.

2. Astra Trident에서 다음을 수행합니다.

   a. 인 각 PV에 대해 스냅샷 디렉토리를 활성화합니다 `ontap-nas-economy` 애플리케이션 기반 및 관련:

   ```
   tridentctl update volume <pv name> --snapshot-dir=true --pool
   -level=true -n trident
   ```

   b. 연결된 각 PV에 대해 스냅샷 디렉토리가 활성화되었는지 확인합니다.

   ```
   tridentctl get volume <pv name> -n trident -o yaml | grep
   snapshotDir
   ```

   응답:

   ```
   snapshotDirectory: "true"
   ```

3. Astra Control에서 연결된 모든 스냅샷 디렉토리를 활성화한 후 애플리케이션을 업데이트하여 Astra Control이 변경된 값을 인식하도록 합니다.

결과

Astra Control을 사용하여 애플리케이션을 백업 및 복원할 준비가 되었습니다. 각 PVC는 백업 및 복원을 위해 다른 응용 프로그램에서 사용할 수도 있습니다.

변경 불가능한 백업을 생성합니다

백업을 저장하는 버킷의 보존 정책에서 금지하는 한 변경 불가능한 백업은 수정, 삭제 또는 덮어쓸 수 없습니다. 보존 정책이 구성된 버킷에 애플리케이션을 백업하여 변경 불가능한 백업을 만들 수 있습니다. 을 참조하십시오 "데이터 보호" 변경 불가능한 백업 작업에 대한 중요한 정보를 참조하십시오.

시작하기 전에

보존 정책을 사용하여 대상 버킷을 구성해야 합니다. 사용하는 스토리지 공급자에 따라 이 방법이 달라집니다. 자세한 내용은 다음 스토리지 제공업체 설명서를 참조하십시오.

- * Amazon Web Services *: "버킷을 생성할 때 S3 오브젝트 잠금을 설정하고 기본 보존 기간으로 기본 보존 모드를 "거버넌스"로 설정합니다".
- * NetApp StorageGRID *: "버킷을 생성할 때 S3 오브젝트 잠금을 설정하고 기본 보존 기간을 사용하여 기본 보존 모드를 "규정 준수"로 설정합니다".

> Astra Control의 버킷은 사용 가능한 용량을 보고하지 않습니다. Astra Control에서 관리되는 앱을 백업 또는 클론 복제하기 전에 적절한 스토리지 관리 시스템에서 버킷 정보를 확인하십시오.

> 앱이 에서 지원하는 저장소 클래스를 사용하는 경우 `ontap-nas-economy` 드라이버, 을(를) 정의했는지 확인하십시오 `backendType` 매개 변수 을 선택합니다 "Kubernetes 스토리지 오브젝트입니다" 을 값으로 사용합니다 `ontap-nas-economy` 보호 작업을 수행하기 전에

단계

1. 응용 프로그램 * 을 선택합니다.
2. 원하는 앱의 * Actions * 열에 있는 옵션 메뉴에서 * Back Up * 을 선택합니다.
3. 백업 이름을 사용자 지정합니다.
4. 기존 스냅샷에서 앱을 백업할지 여부를 선택합니다. 이 옵션을 선택하면 기존 스냅샷 목록에서 선택할 수 있습니다.
5. 스토리지 버킷 목록에서 백업할 대상 버킷을 선택합니다. WORM(Write Once Read Many) 버킷은 버킷 이름 옆에 "잠김" 상태로 표시됩니다.

   > 버켓이 지원되지 않는 유형인 경우 버킷을 가리키거나 선택할 때 표시됩니다.

6. 다음 * 을 선택합니다.
7. 백업 요약을 검토하고 * 백업 * 을 선택합니다.

결과

Astra Control은 앱의 변경 불가능한 백업을 생성한다.

- 네트워크에 정전이 발생했거나 비정상적으로 느린 경우 백업 작업이 시간 초과될 수 있습니다. 이로 인해 백업이 실패합니다.
- 동일한 앱의 변경 불가능한 백업을 두 번 동일한 버킷에 동시에 생성하려는 경우 Astra Control이 두 번째 백업을 시작하지 못합니다. 첫 번째 백업이 완료될 때까지 기다린 후 다른 백업을 시작하십시오.
- 실행 중인 변경 불가능한 백업은 취소할 수 없습니다.
- 데이터 보호 작업(클론, 백업, 복원)과 후속 영구 볼륨 크기 조정 후 UI에 새 볼륨 크기가 표시되기까지 최대 20분이 지연됩니다. 데이터 보호 작업이 몇 분 내에 성공적으로 완료되며 스토리지 백엔드에 관리 소프트웨어를 사용하여 볼륨 크기 변경을 확인할 수 있습니다.

스냅샷 및 백업을 봅니다

Data Protection 탭에서 앱의 스냅샷 및 백업을 볼 수 있습니다.

변경 불가능한 백업은 사용 중인 버킷 옆에 "잠김" 상태로 표시됩니다.

단계

1. 응용 프로그램 * 을 선택한 다음 앱 이름을 선택합니다.
2. 데이터 보호 * 를 선택합니다.

   스냅샷은 기본적으로 표시됩니다.

3. 백업 목록을 보려면 * backups * 를 선택합니다.

스냅샷을 삭제합니다

더 이상 필요하지 않은 예약된 스냅샷 또는 주문형 스냅샷을 삭제합니다.

현재 복제 중인 스냅샷은 삭제할 수 없습니다.

단계

1. 응용 프로그램 * 을 선택한 다음 관리되는 응용 프로그램의 이름을 선택합니다.
2. 데이터 보호 * 를 선택합니다.
3. 원하는 스냅샷에 대한 * Actions * 열의 Options 메뉴에서 * Delete snapshot * 을 선택합니다.
4. 삭제를 확인하려면 "delete"라는 단어를 입력하고 * Yes, Delete snapshot * 을 선택합니다.

결과

Astra Control이 스냅샷을 삭제합니다.

백업을 취소합니다

진행 중인 백업을 취소할 수 있습니다.

백업을 취소하려면 백업이 에 있어야 합니다 `Running` 상태. 에 있는 백업은 취소할 수 없습니다 `Pending` 상태.

실행 중인 변경 불가능한 백업은 취소할 수 없습니다.

단계

1. 응용 프로그램 * 을 선택한 다음 앱 이름을 선택합니다.
2. 데이터 보호 * 를 선택합니다.
3. Backups * 를 선택합니다.
4. 원하는 백업에 대한 * Actions * 열의 Options 메뉴에서 * Cancel * 을 선택합니다.
5. 작업을 확인하려면 "취소"라는 단어를 입력하고 * 예, 백업 취소 * 를 선택합니다.

백업을 삭제합니다

더 이상 필요하지 않은 예약된 백업 또는 필요 시 백업을 삭제합니다. 버켓의 보존 정책을 사용할 수 있을 때까지 변경 불가능한 버킷에 대해 수행된 백업을 삭제할 수 없습니다.

보존 기간이 만료되기 전에는 변경 불가능한 백업을 삭제할 수 없습니다.

실행 중인 백업을 취소해야 하는 경우 의 지침을 따릅니다 백업을 취소합니다. 백업을 삭제하려면 백업이 완료될 때까지 기다린 다음 이 지침을 따르십시오.

단계

1. 응용 프로그램 * 을 선택한 다음 앱 이름을 선택합니다.
2. 데이터 보호 * 를 선택합니다.
3. Backups * 를 선택합니다.
4. 원하는 백업에 대한 * Actions * 열의 Options 메뉴에서 * Delete backup * 을 선택합니다.
5. 삭제를 확인하려면 "delete"라는 단어를 입력하고 * Yes, Delete backup * 을 선택합니다.

결과

Astra Control이 백업을 삭제합니다.

앱 복원

Astra Control은 스냅샷 또는 백업에서 애플리케이션을 복원할 수 있습니다. 애플리케이션을 동일한 클러스터로 복구할 경우 기존 스냅샷에서 복구하는 속도가 빨라집니다. Astra Control UI 또는 를 사용할 수 있습니다 "Astra Control API를 참조하십시오" 앱을 복원합니다.

시작하기 전에

- * 앱을 먼저 보호 *: 복원하기 전에 응용 프로그램의 스냅샷 또는 백업을 수행하는 것이 좋습니다. 이렇게 하면 복구가 실패할 경우 스냅샷 또는 백업에서 클론을 생성할 수 있습니다.
- * 대상 볼륨 확인 *: 다른 스토리지 클래스로 복원하는 경우 스토리지 클래스가 동일한 영구 볼륨 액세스 모드(예:

ReadWriteMany)를 사용하는지 확인합니다. 대상 영구 볼륨 액세스 모드가 다르면 복원 작업이 실패합니다. 예를 들어, 소스 영구 볼륨에서 rwx 액세스 모드를 사용하는 경우 Azure Managed Disks, AWS EBS, Google Persistent Disk 또는 와 같이 rwx를 제공할 수 없는 대상 스토리지 클래스를 선택합니다 `ontap-san`, 복구 작업이 실패합니다. 영구 볼륨 액세스 모드에 대한 자세한 내용은 를 참조하십시오 "쿠버네티스" 문서화:

- * 공간 요구사항 계획 *: NetApp ONTAP 스토리지를 사용하는 애플리케이션의 데이터 이동 없이 복원을 수행할 경우 복원된 앱에서 사용하는 공간이 두 배로 증가할 수 있습니다. 데이터 이동 없이 복구를 수행한 후 복구된 애플리케이션에서 원치 않는 스냅샷을 모두 제거하여 스토리지 공간을 확보합니다.
- * (Red Hat OpenShift 클러스터에만 해당) 정책 추가 *: OpenShift 클러스터에서 앱을 호스팅하기 위한 프로젝트를 생성할 때 프로젝트(또는 Kubernetes 네임스페이스)에 SecurityContext UID가 할당됩니다. Astra Control Center에서 앱을 보호하고 OpenShift의 다른 클러스터 또는 프로젝트로 앱을 이동하려면 해당 앱을 UID로 실행할 수 있는 정책을 추가해야 합니다. 예를 들어 다음 OpenShift CLI 명령은 WordPress 앱에 적절한 정책을 부여합니다.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

- * 지원되는 스토리지 클래스 드라이버 *: Astra Control은 다음 드라이버로 지원되는 스토리지 클래스를 사용하여 백업 복원을 지원합니다.
  - `ontap-nas`
  - `ontap-nas-economy`
  - `ontap-san`
  - `ontap-san-economy`
- * (ONTAP-NAS-이코노미 드라이버만 해당) 백업 및 복원 *: 에서 지원하는 스토리지 클래스를 사용하는 앱을 백업 또는 복원하기 전에 `ontap-nas-economy` 드라이버에서 을 확인합니다 "ONTAP 스토리지 백엔드의 스냅샷 디렉토리가 숨겨집니다". 이 디렉토리를 숨기지 않으면 특히 NFSv3을 사용하는 경우에는 애플리케이션에 대한 액세스가 손실될 수 있습니다.
- * H제어 응용 프로그램 배포 *: Helm 3으로 배포된 응용 프로그램(또는 Helm 2에서 Helm 3으로 업그레이드)이 완벽하게 지원됩니다. Helm 2와 함께 배포된 앱은 지원되지 않습니다.

> 다른 앱과 리소스를 공유하는 앱에서 데이터 이동 없이 복원 작업을 수행하면 의도하지 않은 결과가 발생할 수 있습니다. 앱 간에 공유되는 모든 리소스는 앱 중 하나에서 데이터 이동 없이 복원이 수행될 때 교체됩니다. 자세한 내용은 을 참조하십시오 이 예는 다음과 같습니다.

단계

1. 응용 프로그램 * 을 선택한 다음 앱 이름을 선택합니다.
2. 작업 열의 옵션 메뉴에서 * 복원 * 을 선택합니다.
3. 복원 유형 선택:
   - * 원래 네임스페이스로 복원 *: 이 절차를 사용하여 원래 클러스터로 응용 프로그램을 원래 상태로 복원할 수 있습니다.

> 앱이 에서 지원하는 저장소 클래스를 사용하는 경우 `ontap-nas-economy` 드라이버, 원래 저장소 클래스를 사용하여 앱을 복원해야 합니다. 앱을 동일한 네임스페이스로 복원하는 경우 다른 스토리지 클래스를 지정할 수 없습니다.

   i. 앱을 원래 상태로 복원하는 데 사용할 스냅샷 또는 백업을 선택합니다. 그러면 앱이 이전 버전으로

되돌아갑니다.

ii. 다음 * 을 선택합니다.

> 이전에 삭제된 네임스페이스에 복원하는 경우 복원 프로세스의 일부로 동일한 이름의 새 네임스페이스가 만들어집니다. 이전에 삭제된 네임스페이스에서 앱을 관리할 권한이 있는 사용자는 새로 다시 생성된 네임스페이스에 대한 권한을 수동으로 복원해야 합니다.

◦ * 새 네임스페이스로 복원 *: 이 절차를 사용하여 응용 프로그램을 다른 클러스터나 소스의 다른 네임스페이스로 복원할 수 있습니다.

i. 복원된 앱의 이름을 지정합니다.

ii. 복원하려는 앱의 대상 클러스터를 선택합니다.

iii. 앱과 연결된 각 소스 네임스페이스의 대상 네임스페이스를 입력합니다.

> Astra Control은 이 복원 옵션의 일부로 새 대상 네임스페이스를 만듭니다. 지정한 대상 네임스페이스가 대상 클러스터에 이미 있으면 안 됩니다.

iv. 다음 * 을 선택합니다.

v. 앱을 복원하는 데 사용할 스냅샷 또는 백업을 선택합니다.

vi. 다음 * 을 선택합니다.

vii. 다음 중 하나를 선택합니다.

- * 원래 스토리지 클래스를 사용하여 복원 *: 대상 클러스터에 없는 경우 응용 프로그램은 원래 연결된 스토리지 클래스를 사용합니다. 이 경우 클러스터의 기본 스토리지 클래스가 사용됩니다.
- * 다른 스토리지 클래스를 사용하여 복구 *: 타겟 클러스터에 존재하는 스토리지 클래스를 선택합니다. 원래 연결된 스토리지 클래스에 관계없이 모든 애플리케이션 볼륨은 복구의 일부로 이 서로 다른 스토리지 클래스로 마이그레이션됩니다.

viii. 다음 * 을 선택합니다.

4. 필터링할 자원 선택:

◦ * 모든 리소스 복원 *: 원래 앱과 연결된 모든 리소스를 복원합니다.

◦ * 필터 리소스 *: 원래 응용 프로그램 리소스의 하위 집합을 복원하는 규칙을 지정합니다.

i. 복원된 응용 프로그램에서 리소스를 포함하거나 제외하도록 선택합니다.

ii. 포함 규칙 추가 * 또는 * 제외 규칙 추가 * 를 선택하고 응용 프로그램 복원 중에 올바른 리소스를 필터링하도록 규칙을 구성합니다. 규칙을 편집하거나 제거하고 구성이 올바른지 때까지 규칙을 다시 만들 수 있습니다.

> 포함 및 제외 규칙 구성에 대한 자세한 내용은 을 참조하십시오 응용 프로그램 복원 중에 리소스를 필터링합니다.

5. 다음 * 을 선택합니다.

6. 복원 작업에 대한 세부 정보를 주의 깊게 검토하고 "restore"를 입력하고(메시지가 나타나면) * Restore * 를 선택합니다.

결과

Astra Control은 사용자가 제공한 정보를 기반으로 앱을 복원합니다. 앱을 제자리에 복원한 경우 기존 영구 볼륨의 콘텐츠가 복원된 앱의 영구 볼륨 콘텐츠로 바뀝니다.

데이터 보호 작업(클론, 백업 또는 복원)과 후속 영구 볼륨 크기 조정 후 웹 UI에 새 볼륨 크기가 표시되기까지 최대 20분이 지연됩니다. 데이터 보호 작업이 몇 분 내에 성공적으로 완료되며 스토리지 백엔드에 관리 소프트웨어를 사용하여 볼륨 크기 변경을 확인할 수 있습니다.

네임스페이스 이름/ID 또는 네임스페이스 레이블에 의해 네임스페이스 제한이 있는 구성원 사용자는 동일한 클러스터 또는 조직 계정의 다른 클러스터에 있는 새 네임스페이스에 앱을 클론 복제하거나 복원할 수 있습니다. 그러나 동일한 사용자가 새 네임스페이스에서 복제되거나 복원된 앱에 액세스할 수 없습니다. 클론 또는 복원 작업에서 새 네임스페이스를 생성한 후 계정 관리자/소유자는 구성원 사용자 계정을 편집하고 영향을 받는 사용자의 역할 제약 조건을 업데이트하여 새 네임스페이스에 대한 액세스 권한을 부여할 수 있습니다.

응용 프로그램 복원 중에 리소스를 필터링합니다

에 필터 규칙을 추가할 수 있습니다 "복원" 복원된 응용 프로그램에서 포함하거나 제외할 기존 응용 프로그램 리소스를 지정하는 작업입니다. 지정된 네임스페이스, 레이블 또는 GVK(GroupVersionKind)를 기반으로 리소스를 포함하거나 제외할 수 있습니다.

포함 및 제외 시나리오에 대한 자세한 내용은 를 확장합니다

- * 원본 네임스페이스가 있는 포함 규칙(원본 위치 복원) * 을 선택합니다. 규칙에 정의된 기존 응용 프로그램 리소스는 삭제되며 복구에 사용하는 선택한 스냅숏 또는 백업의 리소스로 대체됩니다. 포함 규칙에 지정하지 않은 모든 리소스는 변경되지 않습니다.
- * 새 네임스페이스가 있는 포함 규칙 선택 *: 이 규칙을 사용하여 복원된 응용 프로그램에서 원하는 특정 리소스를 선택합니다. 포함 규칙에 지정하지 않은 리소스는 복원된 응용 프로그램에 포함되지 않습니다.
- * 원본 네임스페이스가 있는 제외 규칙(원본 위치 복원) * 선택: 제외하도록 지정한 리소스는 복원되지 않고 변경되지 않습니다. 제외하도록 지정하지 않은 리소스는 스냅샷 또는 백업에서 복구됩니다. 해당 StatefulSet 이 필터링된 리소스의 일부인 경우 영구 볼륨의 모든 데이터가 삭제되고 다시 생성됩니다.
- * 새 네임스페이스가 있는 제외 규칙을 선택합니다. * : 규칙을 사용하여 복원된 응용 프로그램에서 제거할 특정 리소스를 선택합니다. 제외하도록 지정하지 않은 리소스는 스냅샷 또는 백업에서 복구됩니다.

규칙은 포함 또는 제외 유형입니다. 자원 포함과 제외 를 결합하는 규칙은 사용할 수 없습니다.

단계

1. 리소스를 필터링하도록 선택하고 앱 복원 마법사에서 포함 또는 제외 옵션을 선택한 후 * 포함 규칙 추가 * 또는 * 제외 규칙 추가 * 를 선택합니다.

   Astra Control에 의해 자동으로 포함되는 클러스터 범위 리소스는 제외할 수 없습니다.

2. 필터 규칙 구성:

   적어도 하나의 네임스페이스, 레이블 또는 GVK를 지정해야 합니다. 필터 규칙을 적용한 후 유지하는 리소스가 복원된 응용 프로그램을 양호한 상태로 유지하는 데 충분한지 확인합니다.

   a. 규칙의 특정 네임스페이스를 선택합니다. 선택하지 않으면 모든 네임스페이스가 필터에 사용됩니다.

응용 프로그램에 원래 여러 네임스페이스가 포함되어 있고 이를 새 네임스페이스로 복원하면 리소스에 포함되지 않은 네임스페이스도 모두 만들어집니다.

b. (선택 사항) 리소스 이름을 입력합니다.

c. (선택 사항) * 라벨 선택기 *: 포함 "라벨 선택기" 규칙에 추가합니다. 레이블 선택기는 선택한 레이블과 일치하는 자원만 필터링하는 데 사용됩니다.

d. (선택 사항) 추가 필터링 옵션을 사용하려면 GVK(GroupVersionKind) SET * 를 선택하여 리소스 * 를 필터링합니다.

GVK 필터를 사용하는 경우 버전 및 종류를 지정해야 합니다.

i. (선택 사항) * Group *: 드롭다운 목록에서 Kubernetes API 그룹을 선택합니다.

ii. * Kind *: 드롭다운 목록에서 필터에 사용할 Kubernetes 리소스 유형에 대한 오브젝트 스키마를 선택합니다.

iii. * 버전 *: Kubernetes API 버전을 선택합니다.

3. 항목에 따라 만들어진 규칙을 검토합니다.

4. 추가 * 를 선택합니다.

원하는 만큼 리소스 포함 및 제외 규칙을 만들 수 있습니다. 작업을 시작하기 전에 복원 애플리케이션 요약에 규칙이 나타납니다.

다른 앱과 리소스를 공유하는 앱의 데이터 이동 없이 복원 복잡성

다른 앱과 리소스를 공유하고 의도하지 않은 결과를 생성하는 앱에서 현재 위치 복원 작업을 수행할 수 있습니다. 앱 간에 공유되는 모든 리소스는 앱 중 하나에서 데이터 이동 없이 복원이 수행될 때 교체됩니다.

다음은 복원에 NetApp SnapMirror 복제를 사용할 때 바람직하지 않은 상황을 만드는 예제 시나리오입니다.

1. 애플리케이션을 정의합니다 `app1` 네임스페이스 사용 `ns1`.
2. 에 대한 복제 관계를 구성합니다 `app1`.
3. 애플리케이션을 정의합니다 `app2` 네임스페이스 사용 `ns1` 및 `ns2`.
4. 에 대한 복제 관계를 구성합니다 `app2`.
5. 에 대한 역방향 복제를 수행합니다 `app2`. 이렇게 하면 가 발생합니다 `app1` 비활성화할 소스 클러스터의 앱.

SnapMirror 기술을 사용하여 스토리지 백엔드 간에 앱을 복제합니다

Astra Control을 사용하면 NetApp SnapMirror 기술의 비동기식 복제 기능을 사용하여 낮은 RPO(복구 시점 목표) 및 낮은 RTO(복구 시간 목표)로 애플리케이션에 대한 비즈니스 연속성을 구축할 수 있습니다. 이 기능을 구성하면 애플리케이션에서 한 스토리지 백엔드에서 다른 스토리지 백엔드, 동일한 클러스터 또는 서로 다른 클러스터 간에 데이터 및 애플리케이션 변경 사항을 복제할 수 있습니다.

백업/복구와 복제를 비교하려면 을 참조하십시오 "데이터 보호 개념".

다음과 같은 사내 전용, 하이브리드 및 멀티 클라우드 시나리오와 같은 다양한 시나리오에서 앱을 복제할 수 있습니다.

- 사내 사이트 A에서 사내 사이트 A로
- 사내 사이트 A에서 사내 사이트 B로
- Cloud Volumes ONTAP를 사용하여 사내에서 클라우드로 전환
- Cloud Volumes ONTAP를 사용하는 클라우드를 사내에서 운영
- Cloud Volumes ONTAP를 사용하는 클라우드(동일한 클라우드 공급자 내의 서로 다른 지역 또는 다른 클라우드 공급자 간)

Astra Control은 사내 클러스터, 사내 클러스터, 클라우드(Cloud Volumes ONTAP 사용) 또는 클라우드 간(Cloud Volumes ONTAP에서 Cloud Volumes ONTAP로) 애플리케이션을 복제할 수 있습니다.

다른 앱을 반대 방향으로 동시에 복제할 수 있습니다. 예를 들어, 애플리케이션 A, B, C를 데이터 센터 1에서 데이터 센터 2로 복제하고 애플리케이션 X, Y, Z를 데이터 센터 2에서 데이터 센터 1로 복제할 수 있습니다.

Astra Control을 사용하면 애플리케이션 복제와 관련된 다음 작업을 수행할 수 있습니다.

- 복제 관계를 설정합니다
- 대상 클러스터에서 복제된 앱을 온라인 상태로 전환(페일오버)
- 페일오버된 복제 다시 동기화
- 애플리케이션 복제를 역으로 수행합니다
- 애플리케이션을 원래 소스 클러스터로 페일백합니다
- 애플리케이션 복제 관계를 삭제합니다

복제 사전 요구 사항

Astra Control 애플리케이션 복제를 시작하려면 먼저 다음과 같은 사전 요구 사항을 충족해야 합니다.

ONTAP 클러스터

- * Astra Trident *: Astra Trident 버전 22.10 이상이 ONTAP를 백엔드로 사용하는 소스 및 대상 Kubernetes 클러스터 모두에 있어야 합니다. Astra Control은 다음 드라이버에서 지원하는 스토리지 클래스를 사용하여 NetApp SnapMirror 기술을 통한 복제를 지원합니다.
  - `ontap-nas`
  - `ontap-san`
- * 라이센스 *: 소스 및 대상 ONTAP 클러스터 모두에서 데이터 보호 번들을 사용하는 ONTAP SnapMirror 비동기 라이센스를 활성화해야 합니다. 을 참조하십시오 "ONTAP의 SnapMirror 라이센스 개요" 를 참조하십시오.

피어링

- * 클러스터 및 SVM *: ONTAP 스토리지 백엔드를 피어링해야 합니다. 을 참조하십시오 "클러스터 및 SVM 피어링 개요" 를 참조하십시오.

두 ONTAP 클러스터 간의 복제 관계에 사용되는 SVM 이름이 고유한지 확인합니다.

- * Astra Trident 및 SVM *: 대상 클러스터의 Astra Trident에서 피어링된 원격 SVM을 사용할 수 있어야 합니다.

Astra 제어 센터

- * 관리되는 백엔드 *: Astra Control Center에서 ONTAP 스토리지 백엔드를 추가 및 관리하여 복제 관계를 생성해야 합니다.

  **Astra Control Provisioner*만 해당 *: Astra Control Center 23.10 이상에 Astra Control Provisioner를 사용하도록 설정한 경우 Astra Control Center에서 ONTAP 스토리지 백엔드를 추가 및 관리하는 것은 선택 사항입니다.

- * 관리되는 클러스터 *: Astra Control을 사용하여 다음 클러스터를 추가하고 관리하는데, 이상적으로는 다른 장애 도메인 또는 사이트에서 사용할 수 있습니다.
  - 소스 Kubernetes 클러스터
  - 대상 Kubernetes 클러스터
  - 연결된 ONTAP 클러스터
- * 사용자 계정 *: ONTAP 스토리지 백엔드를 Astra 제어 센터에 추가할 때 "admin" 역할을 사용하여 사용자 자격 증명을 적용합니다. 이 역할에는 액세스 방법이 있습니다 `http` 및 `ontapi` ONTAP 소스 클러스터와 대상 클러스터 모두에서 사용하도록 설정되었습니다. 을 참조하십시오 "ONTAP 설명서에서 사용자 계정을 관리합니다" 를 참조하십시오.

  **Astra Control Provisioner* 전용 *: Astra Control Provisioner 기능을 활성화한 경우 Astra Control Center에서 클러스터를 관리하기 위한 "admin" 역할을 더 이상 구체적으로 정의할 필요가 없습니다. 이러한 자격 증명이 Astra Control Center 내에서 더 이상 필요하지 않습니다.

"Astra Control Center를 구축합니다" 원활한 재해 복구를 위한 세 번째 장애 도메인 또는 보조 사이트.

Astra Control Center는 TCP 프로토콜을 통해 NVMe를 사용하는 스토리지 백엔드에 대해 NetApp SnapMirror 복제를 지원하지 않습니다.

Astra Trident/ONTAP 구성

Astra Control Center를 사용하려면 소스 및 타겟 클러스터 모두에 대한 복제를 지원하는 스토리지 백엔드를 하나 이상 구성해야 합니다. 소스 및 대상 클러스터가 동일한 경우 대상 애플리케이션은 최상의 복원력을 위해 소스 애플리케이션과 다른 스토리지 백엔드를 사용해야 합니다.

Astra Control 복제는 단일 스토리지 클래스를 사용하는 애플리케이션을 지원합니다. 네임스페이스에 앱을 추가하는 경우 네임스페이스에서 다른 앱과 동일한 저장소 클래스가 앱에 있는지 확인합니다. 복제된 앱에 PVC를 추가할 때 새로운 PVC의 저장 클래스가 네임스페이스의 다른 PVC와 동일한지 확인하십시오.

복제 관계를 설정합니다

복제 관계를 설정하려면 다음을 수행해야 합니다.

- Astra Control에서 앱 스냅샷을 얼마나 자주 생성할지 선택(앱의 Kubernetes 리소스 및 각 앱의 볼륨에 대한 볼륨 스냅샷 포함)
- 복제 일정 선택(Kubernetes 리소스 및 영구 볼륨 데이터 포함)

- 스냅샷을 생성할 시간을 설정합니다

단계

1. Astra Control 왼쪽 탐색 모음에서 * 응용 프로그램 * 을 선택합니다.
2. 데이터 보호 * > * 복제 * 탭을 선택합니다.
3. Configure replication policy * 를 선택합니다. 또는 애플리케이션 보호 상자에서 작업 옵션을 선택하고 * 복제 정책 구성 * 을 선택합니다.
4. 다음 정보를 입력하거나 선택합니다.
   - * 대상 클러스터 *: 대상 클러스터를 입력합니다(소스 클러스터와 같을 수 있음).
   - * 대상 스토리지 클래스 *: 대상 ONTAP 클러스터에서 피어링된 SVM을 사용하는 스토리지 클래스를 선택하거나 입력합니다. 모범 사례로서, 대상 스토리지 클래스는 소스 스토리지 클래스와 다른 스토리지 백엔드를 가리켜야 합니다.
   - * 복제 유형 *: `Asynchronous` 은 현재 사용 가능한 유일한 복제 유형입니다.
   - * 대상 네임스페이스 *: 대상 클러스터에 대한 새 또는 기존 대상 네임스페이스를 입력합니다.
   - (선택 사항) * 네임스페이스 추가 * 를 선택하고 드롭다운 목록에서 네임스페이스를 선택하여 네임스페이스를 추가합니다.
   - * 복제 빈도 *: Astra Control이 스냅샷을 촬영하여 대상에 복제할 빈도를 설정합니다.
   - * Offset *: Astra Control에서 스냅샷을 생성할 시간(분)을 설정합니다. 다른 예약된 작업과 일치하지 않도록 오프셋을 사용할 수 있습니다.

     백업 및 복제 일정을 오프셋하여 일정이 겹치지 않도록 합니다. 예를 들어, 매시간 맨 위에서 백업을 수행하고 5분 오프셋 및 10분 간격으로 복제를 시작하도록 예약합니다.
5. 다음 * 을 선택하고 요약을 검토하고 * 저장 * 을 선택합니다.

   첫 번째 일정이 발생하기 전에 상태가 "APP-MIRROR"로 표시됩니다.

   Astra Control은 복제에 사용되는 애플리케이션 스냅샷을 생성합니다.
6. 응용 프로그램 스냅샷 상태를 보려면 * 응용 프로그램 * > * 스냅샷 * 탭을 선택합니다.

   스냅샷 이름은 의 형식을 사용합니다 `replication-schedule-<string>`. Astra Control은 복제에 사용된 마지막 스냅샷을 보존합니다. 복제를 성공적으로 완료한 후에는 이전의 모든 복제 스냅샷이 삭제됩니다.

결과

그러면 복제 관계가 생성됩니다.

Astra Control은 관계를 수립함으로써 다음과 같은 조치를 수행합니다.

- 대상에서 네임스페이스 생성(없는 경우)
- 소스 앱의 PVC에 해당하는 대상 네임스페이스에 PVC를 생성합니다.
- 애플리케이션 정합성이 보장되는 초기 스냅샷을 생성합니다.
- 초기 스냅샷을 사용하여 영구 볼륨의 SnapMirror 관계를 설정합니다.

데이터 보호 * 페이지에는 복제 관계 상태 및 상태가 표시됩니다.
<Health status> | <Relationship life cycle state>

예를 들면 다음과 같습니다.
정상|설정됨

이 항목의 끝에 있는 복제 상태 및 상태에 대해 자세히 알아보십시오.

대상 클러스터에서 복제된 앱을 온라인 상태로 전환(페일오버)

Astra Control을 사용하면 복제된 애플리케이션을 대상 클러스터로 페일오버할 수 있습니다. 이 절차는 복제 관계를 중지하고 대상 클러스터에서 앱을 온라인으로 전환합니다. 이 절차를 수행해도 소스 클러스터에서 앱이 중지되지 않습니다.

단계

1. Astra Control 왼쪽 탐색 모음에서 * 응용 프로그램 * 을 선택합니다.
2. 데이터 보호 * > * 복제 * 탭을 선택합니다.
3. Actions 메뉴에서 * Fail Over * 를 선택합니다.
4. 페일오버 페이지에서 정보를 검토하고 * 페일오버 * 를 선택합니다.

결과

페일오버 절차로 인해 다음 작업이 수행됩니다.

- 대상 앱은 최근 복제된 스냅샷을 기반으로 시작됩니다.
- 소스 클러스터와 앱(작동 중인 경우)이 중지되지 않고 계속 실행됩니다.
- 복제 상태가 "페일오버 중"으로 변경되고, 완료되면 "페일오버 실패"로 변경됩니다.
- 소스 앱의 보호 정책은 페일오버 시 소스 앱에 있는 일정에 따라 대상 앱에 복사됩니다.
- 소스 앱에 복원 후 실행 후크가 하나 이상 활성화된 경우 해당 실행 후크가 대상 앱에 대해 실행됩니다.
- Astra Control은 소스 및 대상 클러스터와 해당 상태 모두에서 앱을 표시합니다.

페일오버된 복제 다시 동기화

재동기화 작업은 복제 관계를 다시 설정합니다. 관계의 소스를 선택하여 소스 또는 타겟 클러스터에 데이터를 유지할 수 있습니다. 이 작업은 SnapMirror 관계를 다시 설정하여 원하는 방향으로 볼륨 복제를 시작합니다.

이 프로세스는 복제를 다시 설정하기 전에 새 대상 클러스터에서 앱을 중지합니다.

재동기화 프로세스 중에 수명 주기 상태가 "설정 중"으로 표시됩니다.

단계

1. Astra Control 왼쪽 탐색 모음에서 * 응용 프로그램 * 을 선택합니다.
2. 데이터 보호 * > * 복제 * 탭을 선택합니다.
3. 작업 메뉴에서 * 재동기화 * 를 선택합니다.
4. 재동기화 페이지에서 보존할 데이터가 포함된 소스 또는 대상 앱 인스턴스를 선택합니다.

대상의 데이터를 덮어쓰므로 재동기화 소스를 신중하게 선택합니다.

5. 계속하려면 * 재동기화 * 를 선택하십시오.
6. "resync"를 입력하여 확인합니다.
7. 예, 재동기화 * 를 선택하여 완료합니다.

결과

- 복제 페이지에는 복제 상태로 "설정 중"이 표시됩니다.
- Astra Control은 새 대상 클러스터에서 애플리케이션을 중지합니다.
- Astra Control은 SnapMirror 재동기화를 사용하여 선택한 방향으로 영구 볼륨 복제를 다시 설정합니다.
- 복제 페이지에는 업데이트된 관계가 표시됩니다.

애플리케이션 복제를 역으로 수행합니다

원래 소스 스토리지 백엔드로 계속 복제하면서 애플리케이션을 대상 스토리지 백엔드로 이동하기 위한 계획된 작업입니다. Astra Control은 대상 앱으로 페일오버하기 전에 소스 애플리케이션을 중지하고 데이터를 대상에 복제합니다.

이 경우 소스와 대상을 스와핑합니다.

단계

1. Astra Control 왼쪽 탐색 모음에서 * 응용 프로그램 * 을 선택합니다.
2. 데이터 보호 * > * 복제 * 탭을 선택합니다.
3. Actions 메뉴에서 * Reverse replication * 을 선택합니다.
4. 역방향 복제 페이지에서 정보를 검토하고 계속하려면 * 역방향 복제 * 를 선택합니다.

결과

역방향 복제의 결과로 다음 작업이 수행됩니다.

- 원본 소스 앱의 Kubernetes 리소스에 대한 스냅샷이 생성됩니다.
- 앱의 Kubernetes 리소스를 삭제하여 원본 소스 앱의 Pod를 정상적으로 중지할 수 있습니다(PVC 및 PVS를 그대로 둡니다).
- 포드가 종료된 후 앱 볼륨의 스냅샷이 촬영되고 복제됩니다.
- SnapMirror 관계가 끊어져 타겟 볼륨이 읽기/쓰기 준비가 되었습니다.
- 앱의 Kubernetes 리소스는 원래 소스 애플리케이션이 종료된 후 복제된 볼륨 데이터를 사용하여 사전 종료 스냅샷에서 복구됩니다.
- 복제는 반대 방향으로 다시 설정됩니다.

애플리케이션을 원래 소스 클러스터로 페일백합니다

Astra Control을 사용하면 다음 작업 시퀀스를 사용하여 장애 조치 작업 후 "장애 복구"를 수행할 수 있습니다. 이 워크플로우에서 원래 복제 방향을 복구하기 위해 Astra Control은 복제 방향을 바꾸기 전에 애플리케이션 변경 사항을 원래 소스 애플리케이션으로 복제(재동기화)합니다.

이 프로세스는 대상에 대한 페일오버를 완료한 관계로부터 시작되며 다음 단계를 포함합니다.

- 페일오버된 상태로 시작합니다.
- 관계를 다시 동기화합니다.
- 복제를 역으로 수행합니다.

단계

1. Astra Control 왼쪽 탐색 모음에서 * 응용 프로그램 * 을 선택합니다.
2. 데이터 보호 * > * 복제 * 탭을 선택합니다.
3. 작업 메뉴에서 * 재동기화 * 를 선택합니다.
4. 페일백 작업의 경우 페일오버된 앱을 재동기화 작업의 소스로 선택합니다(기록된 모든 데이터 유지 사후 페일오버).
5. "resync"를 입력하여 확인합니다.
6. 예, 재동기화 * 를 선택하여 완료합니다.
7. 재동기화가 완료되면 데이터 보호 > 복제 탭의 동작 메뉴에서 * 역방향 복제 * 를 선택합니다.
8. 역방향 복제 페이지에서 정보를 검토하고 * 역방향 복제 * 를 선택합니다.

결과

이렇게 하면 "재동기화" 및 "역관계" 작업의 결과가 결합되어 원래 소스 클러스터에서 애플리케이션이 온라인 상태가 되고 복제가 원래 대상 클러스터로 다시 시작됩니다.

애플리케이션 복제 관계를 삭제합니다

관계를 삭제하면 두 개의 별도 앱이 서로 관계가 없습니다.

단계

1. Astra Control 왼쪽 탐색 모음에서 * 응용 프로그램 * 을 선택합니다.
2. 데이터 보호 * > * 복제 * 탭을 선택합니다.
3. 애플리케이션 보호 상자 또는 관계 다이어그램에서 * 복제 관계 삭제 * 를 선택합니다.

결과

복제 관계를 삭제하면 다음과 같은 작업이 수행됩니다.

- 관계가 설정되었지만 대상 클러스터에서 앱이 아직 온라인 상태가 되지 않은 경우(장애 발생) Astra Control은 초기화 중에 생성된 PVC를 유지하고 "비어 있는" 관리 앱을 대상 클러스터에 남겨두고 생성된 백업을 유지할 수 있도록 대상 앱을 유지합니다.
- 대상 클러스터에서 앱이 온라인 상태가 된 경우(장애 발생), Astra Control은 PVC 및 대상 앱을 유지합니다. 이제 소스 및 대상 앱이 독립 앱으로 취급됩니다. 백업 스케줄은 두 애플리케이션 모두에 유지되지만 서로 연결되지 않습니다.

복제 관계 상태 및 관계 수명 주기 상태입니다

Astra Control은 복제 관계의 관계 상태와 수명 주기의 상태를 표시합니다.

복제 관계 상태

다음 상태는 복제 관계의 상태를 나타냅니다.

- * 정상 *: 관계가 설정되었거나 설정되었으며 최근 스냅샷이 성공적으로 전송되었습니다.
- * 경고 *: 관계가 페일오버되었거나 페일오버되었습니다(따라서 소스 앱을 더 이상 보호하지 않음).
- * 심각 *
  - 관계가 설정 또는 페일오버되고 마지막 조정 시도가 실패했습니다.
  - 관계가 성립되고 새로운 PVC의 추가를 조정하기 위한 마지막 시도가 실패합니다.
  - 관계가 설정되지만(따라서 성공한 스냅샷이 복제되고 페일오버가 가능함) 가장 최근의 스냅샷이 실패했거나 복제하지 못했습니다.

복제 수명 주기 상태입니다

다음 상태는 복제 주기의 여러 단계를 반영합니다.

- * 설정 *: 새 복제 관계가 생성됩니다. Astra Control은 필요한 경우 네임스페이스를 생성하고, 대상 클러스터의 새 볼륨에 지속적인 PVC(Volume Claim)를 생성하여 SnapMirror 관계를 생성합니다. 이 상태는 복제가 재동기화 중이거나 복제 재동기화 중임을 나타낼 수도 있습니다.
- * 설정됨 *: 복제 관계가 있습니다. Astra Control은 주기적으로 PVC가 사용 가능한지 확인하고, 복제 관계를 확인하고, 정기적으로 앱 스냅샷을 생성하고, 앱에서 새로운 PVC 소스를 식별합니다. 이 경우 Astra Control은 복제에 포함할 리소스를 생성합니다.
- * 페일오버 *: Astra Control은 SnapMirror 관계를 중단시키고 마지막으로 성공적으로 복제된 앱 스냅샷에서 앱의 Kubernetes 리소스를 복원합니다.
- * 페일오버됨 *: Astra Control은 소스 클러스터에서 복제를 중지하고, 대상에서 최근(성공한) 복제 앱 스냅샷을 사용하여 Kubernetes 리소스를 복원합니다.
- * 재동기화 *: Astra Control SnapMirror 재동기화를 사용하여 재동기화 소스의 새 데이터를 재동기화 대상으로 재동기화합니다. 이 작업은 동기화 방향에 따라 대상의 일부 데이터를 덮어쓸 수 있습니다. Astra Control은 대상 네임스페이스에서 실행 중인 앱을 중지하고 Kubernetes 앱을 제거합니다. 재동기화 프로세스 중에 상태가 "설정 중"으로 표시됩니다.
- * 후진 *: 은 원래 소스 클러스터로 계속 복제하면서 애플리케이션을 대상 클러스터로 이동하기 위한 계획된 작업입니다. Astra Control은 소스 클러스터에서 애플리케이션을 중지하고, 대상 클러스터에 앱을 페일오버하기 전에 데이터를 대상에 복제합니다. 역방향 복제 중에 상태가 "설정 중"으로 표시됩니다.
- * 삭제 *:
  - 복제 관계가 설정되었지만 아직 페일오버되지 않은 경우 Astra Control은 복제 중에 생성된 PVC를 제거하고 대상 관리 앱을 삭제합니다.
  - 복제가 이미 실패한 경우 Astra Control은 PVC 및 대상 앱을 유지합니다.

애플리케이션 클론 복제 및 마이그레이션

기존 앱을 클론 복제하여 동일한 Kubernetes 클러스터 또는 다른 클러스터에 중복 앱을 생성할 수 있습니다. Astra Control은 앱을 클론할 때 애플리케이션 구성 및 영구 스토리지의 클론을 생성합니다.

Kubernetes 클러스터 간에 애플리케이션 및 스토리지를 이동해야 하는 경우 클로닝에 도움이 될 수 있습니다. 예를

들어, CI/CD 파이프라인과 Kubernetes 네임스페이스 전체에서 워크로드를 이동할 수 있습니다. Astra Control Center UI 또는 를 사용할 수 있습니다 "Astra Control API를 참조하십시오" 앱을 클론 복제 및 마이그레이션합니다.

시작하기 전에

- * 대상 볼륨 확인 *: 다른 스토리지 클래스에 클론을 생성하는 경우 스토리지 클래스가 동일한 영구 볼륨 액세스 모드(예: ReadWriteMany)를 사용하는지 확인합니다. 대상 영구 볼륨 액세스 모드가 다르면 클론 작업이 실패합니다. 예를 들어, 소스 영구 볼륨에서 rwx 액세스 모드를 사용하는 경우 Azure Managed Disks, AWS EBS, Google Persistent Disk 또는 와 같이 rwx를 제공할 수 없는 대상 스토리지 클래스를 선택합니다 `ontap-san`, 클론 작업이 실패합니다. 영구 볼륨 액세스 모드에 대한 자세한 내용은 를 참조하십시오 "쿠버네티스" 문서화:
- 앱을 다른 클러스터에 클론 복제하려면 소스 및 대상 클러스터가 포함된 클라우드 인스턴스(동일하지 않은 경우)에 기본 버킷이 있는지 확인해야 합니다. 각 클라우드 인스턴스에 대해 기본 버킷을 할당해야 합니다.
- 클론 작업 중에 IngressClass 리소스 또는 Webhook가 필요한 애플리케이션에는 대상 클러스터에 이미 정의된 리소스가 없어야 합니다.

OpenShift 환경에서 앱을 복제하는 동안, Astra Control Center는 OpenShift가 볼륨을 마운트하고 파일 소유권을 변경할 수 있도록 허용해야 합니다. 따라서 이러한 작업을 허용하려면 ONTAP 볼륨 내보내기 정책을 구성해야 합니다. 다음 명령을 사용하여 이 작업을 수행할 수 있습니다.

1. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -superuser sys`
2. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -anon 65534`

클론 제한 사항

- * 명시적 스토리지 클래스 *: 스토리지 클래스가 명시적으로 설정된 앱을 배포하고 앱을 복제해야 하는 경우 타겟 클러스터에 원래 지정된 스토리지 클래스가 있어야 합니다. 명시적으로 설정된 스토리지 클래스를 가진 애플리케이션을 동일한 스토리지 클래스가 없는 클러스터로 클론 복제하면 실패합니다.
- * ONTAP - NAS - 경제적인 응용 프로그램 *: 응용 프로그램의 저장소 클래스가 에서 지원될 경우 복제 작업을 사용할 수 없습니다 `ontap-nas-economy` 드라이버. 그러나, "ONTAP - NAS - 경제성 작업을 위한 백업 및 복원 지원".
- * 클론 및 사용자 제약 조건 *: 네임스페이스 이름/ID 또는 네임스페이스 레이블에 의해 네임스페이스 제한이 있는 구성원 사용자는 동일한 클러스터의 새 네임스페이스 또는 조직 계정의 다른 클러스터에 앱을 클론 복제하거나 복원할 수 있습니다. 그러나 동일한 사용자가 새 네임스페이스에서 복제되거나 복원된 앱에 액세스할 수 없습니다. 클론 또는 복원 작업에서 새 네임스페이스를 생성한 후 계정 관리자/소유자는 구성원 사용자 계정을 편집하고 영향을 받는 사용자의 역할 제약 조건을 업데이트하여 새 네임스페이스에 대한 액세스 권한을 부여할 수 있습니다.
- * 클론은 기본 버킷 사용 *: 애플리케이션 백업 또는 애플리케이션 복구 중에 버킷 ID를 선택적으로 지정할 수 있습니다. 그러나 애플리케이션 클론 작업에서는 항상 정의된 기본 버킷을 사용합니다. 클론의 버킷을 변경할 수 있는 옵션은 없습니다. 어떤 버킷이 사용되는지 제어하려는 경우 이 두 가지 방법을 사용할 수 있습니다 "버킷 기본값을 변경합니다" 또는 을 수행합니다 "백업" 뒤에 가 있습니다 "복원" 별도.
- * Jenkins CI * 사용: Jenkins CI의 운영자 배포 인스턴스를 복제하는 경우 영구 데이터를 수동으로 복원해야 합니다. 이는 앱 배포 모델의 제한 사항입니다.
- * S3 버킷 포함 *: Astra Control Center의 S3 버킷은 가용 용량을 보고하지 않습니다. Astra Control Center에서 관리하는 앱을 백업 또는 클론 생성하기 전에 ONTAP 또는 StorageGRID 관리 시스템에서 버킷 정보를 확인하십시오.
- * 특정 버전의 PostgreSQL * 사용: 동일한 클러스터 내의 앱 클론은 Bitnami PostgreSQL 11.5.0 차트와 함께 일관되게 실패합니다. 클론을 성공적으로 생성하려면 이전 또는 이후 버전의 차트를 사용하십시오.

OpenShift 고려 사항

- * 클러스터 및 OpenShift 버전 *: 클러스터 간에 앱을 복제하는 경우 소스 및 대상 클러스터는 OpenShift의 배포와 동일해야 합니다. 예를 들어 OpenShift 4.7 클러스터에서 앱을 클론하는 경우 OpenShift 4.7인 대상 클러스터를 사용합니다.
- * 프로젝트 및 UID *: OpenShift 클러스터에서 앱을 호스팅하기 위한 프로젝트를 생성하면 프로젝트(또는 Kubernetes 네임스페이스)에 SecurityContext UID가 할당됩니다. Astra Control Center에서 앱을 보호하고 OpenShift의 다른 클러스터 또는 프로젝트로 앱을 이동하려면 해당 앱을 UID로 실행할 수 있는 정책을 추가해야 합니다. 예를 들어 다음 OpenShift CLI 명령은 WordPress 앱에 적절한 정책을 부여합니다.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

단계

1. 응용 프로그램 * 을 선택합니다.
2. 다음 중 하나를 수행합니다.
   - 원하는 앱의 * Actions * 열에서 Options 메뉴를 선택합니다.
   - 원하는 앱의 이름을 선택하고 페이지 오른쪽 상단의 상태 드롭다운 목록을 선택합니다.
3. 클론 * 을 선택합니다.
4. 클론의 세부 정보 지정:
   - 이름을 입력합니다.
   - 클론의 대상 클러스터를 선택합니다.
   - 클론의 대상 네임스페이스를 입력합니다. 앱과 연결된 각 소스 네임스페이스는 사용자가 정의하는 대상 네임스페이스에 매핑됩니다.

     Astra Control은 클론 작업의 일부로 새 대상 네임스페이스를 생성합니다. 지정한 대상 네임스페이스가 대상 클러스터에 이미 있으면 안 됩니다.

   - 다음 * 을 선택합니다.
   - 앱과 연결된 원래 저장소 클래스를 유지하거나 다른 저장소 클래스를 선택합니다.

     앱의 스토리지 클래스를 기본 클라우드 공급자 스토리지 클래스나 기타 지원되는 스토리지 클래스로 마이그레이션하고 에서 지원하는 스토리지 클래스에서 앱을 마이그레이션할 수 있습니다 `ontap-nas-economy` 에서 지원하는 스토리지 클래스로 `ontap-nas` 또는 에서 지원하는 저장소 클래스가 있는 다른 클러스터로 앱을 복사합니다 `ontap-nas-economy` 드라이버.

     다른 스토리지 클래스를 선택했고 복원 시 이 스토리지 클래스가 존재하지 않는 경우 오류가 반환됩니다.

5. 다음 * 을 선택합니다.
6. 클론에 대한 정보를 검토하고 * Clone * 을 선택합니다.

결과

Astra Control은 사용자가 제공한 정보를 기반으로 앱을 복제합니다. 새 애플리케이션 클론이 에 있을 때 클론 작업이 성공적으로 수행됩니다 `Healthy` 상태를 표시합니다.

클론 또는 복원 작업에서 새 네임스페이스를 생성한 후 계정 관리자/소유자는 구성원 사용자 계정을 편집하고 영향을 받는 사용자의 역할 제약 조건을 업데이트하여 새 네임스페이스에 대한 액세스 권한을 부여할 수 있습니다.

데이터 보호 작업(클론, 백업 또는 복원)과 후속 영구 볼륨 크기 조정 후 UI에 새 볼륨 크기가 표시되기까지 최대 20분이 지연됩니다. 데이터 보호 작업이 몇 분 내에 성공적으로 완료되며 스토리지 백엔드에 관리 소프트웨어를 사용하여 볼륨 크기 변경을 확인할 수 있습니다.

앱 실행 후크 관리

실행 후크는 관리되는 앱의 데이터 보호 작업과 함께 실행되도록 구성할 수 있는 사용자 지정 작업입니다. 예를 들어 데이터베이스 앱이 있는 경우 실행 후크를 사용하여 스냅샷 전에 모든 데이터베이스 트랜잭션을 일시 중지하고 스냅샷이 완료된 후 트랜잭션을 다시 시작할 수 있습니다. 따라서 애플리케이션 정합성이 보장되는 스냅샷이 보장됩니다.

실행 후크 유형

Astra Control Center는 실행 가능한 시점을 기준으로 다음과 같은 유형의 실행 후크를 지원합니다.

- 사전 스냅샷
- 사후 스냅샷
- 사전 백업
- 백업 후
- 사후 복원
- 장애 조치 후

실행 후크 필터

실행 후크를 응용 프로그램에 추가하거나 편집할 때 실행 후크에 필터를 추가하여 후크가 일치시킬 컨테이너를 관리할 수 있습니다. 필터는 모든 컨테이너에서 동일한 컨테이너 이미지를 사용하는 응용 프로그램에 유용하지만 각 이미지를 다른 용도(예: Elasticsearch)로 사용할 수 있습니다. 필터를 사용하면 실행 후크가 실행되는 시나리오를 만들 수 있습니다. 단, 모든 동일한 컨테이너를 실행하는 것은 아닙니다. 단일 실행 후크에 대해 여러 개의 필터를 만들면 논리적 필터 및 연산자와 결합됩니다. 실행 후크당 최대 10개의 활성 필터를 사용할 수 있습니다.

실행 후크에 추가하는 각 필터는 클러스터의 컨테이너와 일치시키기 위해 정규식을 사용합니다. 후크가 컨테이너와 일치하면 후크는 해당 컨테이너에서 연결된 스크립트를 실행합니다. 필터에 대한 정규식은 정규식 2(RE2) 구문을 사용합니다. 이 구문은 일치 목록에서 컨테이너를 제외하는 필터를 만드는 것을 지원하지 않습니다. Astra Control이 실행 후크 필터의 정규식에 대해 지원하는 구문에 대한 자세한 내용은 을 참조하십시오 "정규식 2(RE2) 구문 지원".

복원 또는 클론 작업 후에 실행되는 실행 후크에 네임스페이스 필터를 추가하고 복원 또는 클론 소스와 대상이 서로 다른 네임스페이스에 있는 경우 네임스페이스 필터는 대상 네임스페이스에만 적용됩니다.

사용자 정의 실행 후크에 대한 중요 참고 사항

앱에 대한 실행 후크를 계획할 때 다음 사항을 고려하십시오.

> 실행 후크는 실행 중인 응용 프로그램의 기능을 줄이거나 완전히 비활성화하기 때문에 사용자 지정 실행 후크가 실행되는 시간을 최소화해야 합니다.
> 연결된 실행 후크와 함께 백업 또는 스냅샷 작업을 시작한 다음 취소하면 백업 또는 스냅샷 작업이 이미 시작된 경우에도 후크를 실행할 수 있습니다. 즉, 백업 후 실행 후크에 사용되는 논리는 백업이 완료된 것으로 가정할 수 없습니다.

- 새 Astra Control 구축 환경에서는 실행 후크 기능이 기본적으로 비활성화되어 있습니다.
  - 실행 후크를 사용하려면 먼저 실행 후크 기능을 활성화해야 합니다.
  - 소유자 또는 관리자 사용자는 현재 Astra Control 계정에 정의된 모든 사용자에 대해 실행 후크 기능을 활성화하거나 비활성화할 수 있습니다. 을 참조하십시오 실행 후크 기능을 활성화합니다 및 실행 후크 기능을 비활성화합니다 를 참조하십시오.
  - Astra Control 업그레이드 중에 기능 지원 상태가 유지됩니다.
- 실행 후크는 스크립트를 사용하여 작업을 수행해야 합니다. 많은 실행 후크가 동일한 스크립트를 참조할 수 있습니다.
- Astra Control에는 실행 후크가 실행 가능한 셸 스크립트 형식으로 기록하는 데 사용하는 스크립트가 필요합니다.
- 스크립트 크기는 96KB로 제한됩니다.
- Astra Control은 실행 후크 설정과 모든 일치 기준을 사용하여 스냅샷, 백업 또는 복구 작업에 적용할 수 있는 후크를 결정합니다.
- 모든 실행 후크 장애는 소프트 장애이며, 후크가 실패하더라도 다른 후크와 데이터 보호 작업은 계속 시도됩니다. 그러나 후크가 실패하면 * Activity * 페이지 이벤트 로그에 경고 이벤트가 기록됩니다.
- 실행 후크를 생성, 편집 또는 삭제하려면 소유자, 관리자 또는 구성원 권한이 있는 사용자여야 합니다.
- 실행 후크를 실행하는 데 25분 이상 걸리는 경우 후크에 장애가 발생하고 반환 코드가 "N/A"인 이벤트 로그 항목이 생성됩니다. 영향을 받는 모든 스냅샷은 시간 초과되어 실패로 표시되며, 그 결과 이벤트 로그 항목이 시간 초과를 나타냅니다.
- 임시 데이터 보호 작업의 경우 모든 후크 이벤트가 생성되고 * Activity * 페이지 이벤트 로그에 저장됩니다. 그러나 예약된 데이터 보호 작업의 경우 후크 장애 이벤트만 이벤트 로그에 기록됩니다(예약된 데이터 보호 작업 자체에서 생성되는 이벤트는 계속 기록됨).
- Astra Control Center가 복제된 소스 앱을 대상 앱으로 페일오버하면 페일오버가 완료된 후 소스 앱에 대해 활성화된 장애 조치 후 실행 후크가 대상 앱에 대해 실행됩니다.

> Astra Control Center 23.04에서 복원 후 후크를 실행하고 Astra Control Center를 23.07 이상으로 업그레이드한 경우 페일오버 복제 후 복원 후 실행 후크가 더 이상 실행되지 않습니다. 앱을 위한 새로운 장애 조치 후 실행 후크를 만들어야 합니다. 또는 "사후 복원"에서 "사후 페일오버 "로 페일오버하기 위한 기존 복원 후 후크의 작업 유형을 변경할 수 있습니다.

실행 순서

데이터 보호 작업이 실행되면 실행 후크 이벤트가 다음 순서로 발생합니다.

1. 해당되는 모든 사용자 정의 사전 작업 실행 후크는 해당 컨테이너에서 실행됩니다. 필요한 만큼 사용자 지정 사전 작업 후크를 만들고 실행할 수 있지만, 이 후크의 실행 순서는 보장되거나 구성할 수 없습니다.

2. 데이터 보호 작업이 수행됩니다.
3. 해당되는 모든 사용자 지정 작업 후 실행 후크는 해당 컨테이너에서 실행됩니다. 필요한 만큼 사용자 지정 사후 작업 후크를 만들고 실행할 수 있지만 작업 후 후크의 실행 순서는 보장되거나 구성할 수 없습니다.

같은 유형의 실행 후크를 여러 개 생성하는 경우(예: 사전 스냅샷) 해당 후크의 실행 순서는 보장되지 않습니다. 그러나 다른 유형의 후크를 실행하는 순서는 보장됩니다. 예를 들어, 서로 다른 모든 유형의 후크가 있는 구성의 실행 순서는 다음과 같습니다.

1. 예비 후크가 실행되었습니다
2. 사전 스냅샷 후크가 실행되었습니다
3. 사후 스냅샷 후크가 실행되었습니다
4. 백업 후 후크가 실행되었습니다
5. 복원 후 후크가 실행되었습니다

시나리오 번호 2에서 이 구성의 예를 볼 수 있습니다 후크가 실행될지 여부를 결정합니다.

운영 환경에서 실행 후크 스크립트를 사용하려면 항상 해당 스크립트를 테스트해야 합니다. 'kubbeck exec' 명령을 사용하여 스크립트를 편리하게 테스트할 수 있습니다. 운영 환경에서 실행 후크를 사용하도록 설정한 후 결과 스냅샷과 백업을 테스트하여 정합성이 보장되는지 확인합니다. 앱을 임시 네임스페이스에 클론 복제하고, 스냅샷 또는 백업을 복원한 다음 앱을 테스트하여 이 작업을 수행할 수 있습니다.

후크가 실행될지 여부를 결정합니다

다음 표를 사용하여 사용자 지정 실행 후크가 앱에 대해 실행되는지 여부를 확인할 수 있습니다.

모든 상위 수준 앱 작업은 스냅샷, 백업 또는 복원의 기본 작업 중 하나를 실행하는 것으로 구성됩니다. 시나리오에 따라 클론 작업은 이러한 작업의 다양한 조합으로 구성되므로 클론 작업이 실행되는 실행 후크는 달라집니다.

데이터 이동 없이 복원 작업을 수행하려면 기존 스냅샷 또는 백업이 필요하므로 이러한 작업은 스냅샷 또는 백업 후크를 실행하지 않습니다.

를 시작한 다음 스냅샷이 포함된 백업을 취소하고 연결된 실행 후크가 있는 경우 일부 후크가 실행될 수 있고 그렇지 않은 백업이 있을 수 있습니다. 즉, 백업 후 실행 후크는 백업이 완료된 것으로 가정할 수 없습니다. 연결된 실행 후크와 함께 취소된 백업의 경우 다음 사항에 유의하십시오.

- 예비 백업 및 예비 후크는 항상 실행됩니다.
- 백업에 새 스냅샷이 포함되어 있고 스냅샷이 시작된 경우 사전 스냅샷 및 사후 스냅샷 후크가 실행됩니다.
- 스냅샷을 시작하기 전에 백업을 취소하면 사전 스냅샷 및 사후 스냅샷 후크가 실행되지 않습니다.

시나리오	작동	기존 스냅샷	더 많은 워크로드 추가/제거	네임스페이스	클러스터	스냅샷 후크가 실행됩니다	백업 후크가 실행됩니다	후크 실행을 복원합니다	페일오버 후크가 실행됩니다
1	복제	해당 없음	해당 없음	신규	동일합니다	예	해당 없음	예	해당 없음

시나리오	작동	기존 스냅샷	더 많은 워크로드 추가/제거	네임스페이스	클러스터	스냅샷 후크가 실행됩니다	백업 후크가 실행됩니다	후크 실행을 복원합니다	페일오버 후크가 실행됩니다
2	복제	해당 없음	해당 없음	신규	다릅니다	예	예	예	해당 없음
3	복제 또는 복원	예	해당 없음	신규	동일합니다	해당 없음	해당 없음	예	해당 없음
4	복제 또는 복원	해당 없음	예	신규	동일합니다	해당 없음	해당 없음	예	해당 없음
5	복제 또는 복원	예	해당 없음	신규	다릅니다	해당 없음	해당 없음	예	해당 없음
6	복제 또는 복원	해당 없음	예	신규	다릅니다	해당 없음	해당 없음	예	해당 없음
7	복원	예	해당 없음	기존	동일합니다	해당 없음	해당 없음	예	해당 없음
8	복원	해당 없음	예	기존	동일합니다	해당 없음	해당 없음	예	해당 없음
9	스냅샷	해당 없음	해당 없음	해당 없음	해당 없음	예	해당 없음	해당 없음	해당 없음
10	백업	해당 없음	해당 없음	해당 없음	해당 없음	예	예	해당 없음	해당 없음
11	백업	예	해당 없음	해당 없음	해당 없음	해당 없음	해당 없음	해당 없음	해당 없음
12	페일오버	예	해당 없음	복제에 의해 생성되었습니다	다릅니다	해당 없음	해당 없음	해당 없음	예
13	페일오버	예	해당 없음	복제에 의해 생성되었습니다	동일합니다	해당 없음	해당 없음	해당 없음	예

실행 후크 예

를 방문하십시오 "NetApp Verda GitHub 프로젝트" Apache Cassandra 및 Elasticsearch와 같은 인기 있는 앱의 실제 실행 후크를 다운로드하려면 다음을 수행합니다. 예제를 보고 사용자 지정 실행 후크를 구조화하는 아이디어를 얻을 수도 있습니다.

실행 후크 기능을 활성화합니다

소유자 또는 관리자 사용자인 경우 실행 후크 기능을 활성화할 수 있습니다. 이 기능을 활성화하면 이 Astra Control 계정에 정의된 모든 사용자가 실행 후크를 사용하고 기존 실행 후크와 후크 스크립트를 볼 수 있습니다.

단계

1. 응용 프로그램 * 으로 이동한 다음 관리되는 응용 프로그램의 이름을 선택합니다.
2. Execution hook * 탭을 선택합니다.
3. 실행 후크 활성화 * 를 선택합니다.

   계정 * > * 기능 설정 * 탭이 나타납니다.

4. Execution Hooks * 창에서 설정 메뉴를 선택합니다.
5. 활성화 * 를 선택합니다.
6. 나타나는 보안 경고를 확인합니다.
7. Yes, enable execution hook * 를 선택합니다.

실행 후크 기능을 비활성화합니다

소유자 또는 관리자 사용자인 경우 이 Astra Control 계정에 정의된 모든 사용자에 대해 실행 후크 기능을 비활성화할 수 있습니다. 실행 후크 기능을 비활성화하려면 먼저 기존 실행 후크를 모두 삭제해야 합니다. 을 참조하십시오 실행 후크를 삭제합니다 기존 실행 후크를 삭제하는 방법에 대한 지침은 을 참조하십시오.

단계

1. 계정 * 으로 이동한 다음 * 기능 설정 * 탭을 선택합니다.
2. Execution hook * 탭을 선택합니다.
3. Execution Hooks * 창에서 설정 메뉴를 선택합니다.
4. 비활성화 * 를 선택합니다.
5. 나타나는 경고를 확인합니다.
6. 유형 `disable` 모든 사용자에 대해 이 기능을 사용하지 않도록 설정할 것인지 확인합니다.
7. 예, 사용 안 함 * 을 선택합니다.

기존 실행 후크를 봅니다

앱의 기존 사용자 지정 실행 후크를 볼 수 있습니다.

단계

1. 응용 프로그램 * 으로 이동한 다음 관리되는 응용 프로그램의 이름을 선택합니다.
2. Execution hook * 탭을 선택합니다.

   결과 목록에서 사용 가능하거나 비활성화된 실행 후크를 모두 볼 수 있습니다. 후크의 상태, 일치하는 컨테이너 수, 생성 시간 및 실행 시간(사전 또는 사후 작업)을 확인할 수 있습니다. 를 선택할 수 있습니다 + 실행할 컨테이너 목록을 확장하려면 후크 이름 옆에 있는 아이콘을 클릭합니다. 이 응용 프로그램의 실행 후크를 둘러싼 이벤트 로그를 보려면 * Activity * 탭으로 이동하십시오.

기존 스크립트 보기

업로드된 기존 스크립트를 볼 수 있습니다. 또한 이 페이지에서 사용 중인 스크립트와 해당 스크립트를 사용하는 후크를 확인할 수 있습니다.

단계

1. 계정 * 으로 이동합니다.
2. 스크립트 * 탭을 선택합니다.

   이 페이지에서는 업로드된 기존 스크립트 목록을 볼 수 있습니다. Used By* 열에는 각 스크립트를 사용하는 실행 후크가 표시됩니다.

스크립트를 추가합니다

각 실행 후크는 스크립트를 사용하여 작업을 수행해야 합니다. 실행 후크가 참조할 수 있는 스크립트를 하나 이상 추가할 수 있습니다. 많은 실행 후크가 동일한 스크립트를 참조할 수 있으므로 하나의 스크립트만 변경하여 여러 실행 후크를 업데이트할 수 있습니다.

단계

1. 실행 후크 기능이 인지 확인합니다 활성화됨.
2. 계정 * 으로 이동합니다.
3. 스크립트 * 탭을 선택합니다.
4. 추가 * 를 선택합니다.
5. 다음 중 하나를 수행합니다.
   - 사용자 지정 스크립트를 업로드합니다.
     i. 파일 업로드 * 옵션을 선택합니다.
     ii. 파일을 찾아 업로드합니다.
     iii. 스크립트에 고유한 이름을 지정합니다.
     iv. (선택 사항) 다른 관리자가 스크립트에 대해 알아야 하는 참고 사항을 입력합니다.
     v. Save script * 를 선택합니다.
   - 클립보드에서 사용자 정의 스크립트를 붙여 넣습니다.
     i. 붙여넣기 또는 형식 * 옵션을 선택합니다.
     ii. 텍스트 필드를 선택하고 필드에 스크립트 텍스트를 붙여 넣습니다.
     iii. 스크립트에 고유한 이름을 지정합니다.
     iv. (선택 사항) 다른 관리자가 스크립트에 대해 알아야 하는 참고 사항을 입력합니다.
6. Save script * 를 선택합니다.

결과

새 스크립트가 * 스크립트 * 탭의 목록에 나타납니다.

스크립트를 삭제합니다

스크립트가 더 이상 필요하지 않고 실행 후크에서 사용되지 않는 경우 시스템에서 스크립트를 제거할 수 있습니다.

단계

1. 계정 * 으로 이동합니다.
2. 스크립트 * 탭을 선택합니다.
3. 제거할 스크립트를 선택하고 * Actions * 열에서 메뉴를 선택합니다.
4. 삭제 * 를 선택합니다.

> ⓘ 스크립트가 하나 이상의 실행 후크에 연결되어 있으면 * 삭제 * 작업을 사용할 수 없습니다. 스크립트를 삭제하려면 먼저 연결된 실행 후크를 편집하여 다른 스크립트에 연결합니다.

사용자 지정 실행 후크를 만듭니다

앱에 대한 사용자 정의 실행 후크를 생성하여 Astra Control에 추가할 수 있습니다. 을 참조하십시오 실행 후크 예 후크 예 실행 후크를 만들려면 소유자, 관리자 또는 구성원 권한이 있어야 합니다.

> 실행 후크로 사용할 사용자 정의 쉘 스크립트를 작성할 때는 특정 명령을 실행하거나 실행 파일에 대한 전체 경로를 제공하지 않는 한 파일 시작 부분에 적절한 셸을 지정해야 합니다.

단계

1. 실행 후크 기능이 인지 확인합니다 활성화됨.
2. 응용 프로그램 * 을 선택한 다음 관리되는 응용 프로그램의 이름을 선택합니다.
3. Execution hook * 탭을 선택합니다.
4. 추가 * 를 선택합니다.
5. 후크 세부 정보 * 영역에서:
   a. 작업 * 드롭다운 메뉴에서 작업 유형을 선택하여 후크를 언제 실행해야 하는지 결정합니다.
   b. 후크의 고유한 이름을 입력합니다.
   c. (선택 사항) 실행 중에 후크에 전달할 인수를 입력하고 각 인수 뒤에 Enter 키를 눌러 각 인수를 기록합니다.
6. (선택 사항) * Hook Filter Details * 영역에서 실행 후크가 실행되는 컨테이너를 제어하는 필터를 추가할 수 있습니다.
   a. 필터 추가 * 를 선택합니다.
   b. Hook filter type * 열의 드롭다운 메뉴에서 필터링할 특성을 선택합니다.
   c. Regex * 열에 필터로 사용할 정규식을 입력합니다. Astra Control은 를 사용합니다 "정규식 2(RE2) regex 구문".

      > 정규식 필드에 다른 텍스트가 없는 특성(예: pod 이름)의 정확한 이름을 필터링하면 부분 문자열 일치가 수행됩니다. 정확한 이름과 해당 이름만 일치시키려면 정확한 문자열 일치 구문(예: `^exact_podname$`)를 클릭합니다.

   d. 필터를 더 추가하려면 * 필터 추가 * 를 선택합니다.

      > 실행 후크에 대한 여러 필터가 논리 및 연산자와 결합됩니다. 실행 후크당 최대 10개의 활성 필터를 사용할 수 있습니다.

7. 완료되면 * Next * 를 선택합니다.
8. Script * 영역에서 다음 중 하나를 수행합니다.
   - 새 스크립트를 추가합니다.
     i. 추가 * 를 선택합니다.
     ii. 다음 중 하나를 수행합니다.
       - 사용자 지정 스크립트를 업로드합니다.
         I. 파일 업로드 * 옵션을 선택합니다.
         II. 파일을 찾아 업로드합니다.

III. 스크립트에 고유한 이름을 지정합니다.

IV. (선택 사항) 다른 관리자가 스크립트에 대해 알아야 하는 참고 사항을 입력합니다.

V. Save script * 를 선택합니다.

- 클립보드에서 사용자 정의 스크립트를 붙여 넣습니다.
  I. 붙여넣기 또는 형식 * 옵션을 선택합니다.
  II. 텍스트 필드를 선택하고 필드에 스크립트 텍스트를 붙여 넣습니다.
  III. 스크립트에 고유한 이름을 지정합니다.
  IV. (선택 사항) 다른 관리자가 스크립트에 대해 알아야 하는 참고 사항을 입력합니다.

◦ 목록에서 기존 스크립트를 선택합니다.

이렇게 하면 실행 후크에 이 스크립트를 사용하도록 지시합니다.

9. 다음 * 을 선택합니다.
10. 실행 후크 구성을 검토합니다.
11. 추가 * 를 선택합니다.

실행 후크의 상태를 확인합니다

스냅샷, 백업 또는 복원 작업이 실행된 후에 작업의 일부로 실행된 실행 후크의 상태를 확인할 수 있습니다. 이 상태 정보를 사용하여 실행 후크를 유지할지, 수정하거나 삭제할 것인지 결정할 수 있습니다.

단계

1. 응용 프로그램 * 을 선택한 다음 관리되는 응용 프로그램의 이름을 선택합니다.
2. 데이터 보호 * 탭을 선택합니다.
3. 스냅샷 * 을 선택하여 실행 중인 스냅샷을 보거나 * 백업 * 을 선택하여 실행 중인 백업을 확인합니다.

   후크 상태 * 는 작업이 완료된 후 실행 후크의 상태를 표시합니다. 상태 위로 마우스를 가져가면 자세한 정보를 볼 수 있습니다. 예를 들어, 스냅샷 중에 실행 후크 오류가 발생한 경우 해당 스냅샷의 후크 상태 위로 마우스를 이동하면 실패한 실행 후크 목록이 표시됩니다. 각 오류의 원인을 확인하려면 왼쪽 탐색 영역의 * Activity * 페이지를 확인하십시오.

스크립트 사용을 봅니다

Astra Control 웹 UI에서 특정 스크립트를 사용하는 실행 후크를 확인할 수 있습니다.

단계

1. 계정 * 을 선택합니다.
2. 스크립트 * 탭을 선택합니다.

   스크립트 목록의 * Used By * 열에 목록의 각 스크립트를 사용하는 후크에 대한 세부 정보가 포함되어 있습니다.

3. 관심 있는 스크립트에 대해 * Used By *(사용 대상 *) 열에서 정보를 선택합니다.

   스크립트를 사용하는 후크의 이름 및 스크립트를 실행하도록 구성된 작업 유형과 함께 더 자세한 목록이

나타납니다.

실행 후크를 편집합니다

실행 후크를 편집하여 속성, 필터 또는 사용하는 스크립트를 변경할 수 있습니다. 실행 후크를 편집하려면 소유자, 관리자 또는 구성원 권한이 있어야 합니다.

단계

1. 응용 프로그램 * 을 선택한 다음 관리되는 응용 프로그램의 이름을 선택합니다.
2. Execution hook * 탭을 선택합니다.
3. 편집할 후크의 경우 * Actions * 열에서 옵션 메뉴를 선택합니다.
4. 편집 * 을 선택합니다.
5. 필요한 사항을 변경하고 각 섹션을 완료한 후 * 다음 * 을 선택합니다.
6. 저장 * 을 선택합니다.

실행 후크를 비활성화합니다

앱 스냅샷 전후에 실행 후크가 실행되지 않도록 임시로 설정하려면 실행 후크를 사용하지 않도록 설정할 수 있습니다. 실행 후크를 비활성화하려면 소유자, 관리자 또는 구성원 권한이 있어야 합니다.

단계

1. 응용 프로그램 * 을 선택한 다음 관리되는 응용 프로그램의 이름을 선택합니다.
2. Execution hook * 탭을 선택합니다.
3. 비활성화할 후크의 경우 * Actions * 열에서 옵션 메뉴를 선택합니다.
4. 비활성화 * 를 선택합니다.

실행 후크를 삭제합니다

더 이상 필요 없는 경우 실행 후크를 완전히 제거할 수 있습니다. 실행 후크를 삭제하려면 소유자, 관리자 또는 구성원 권한이 있어야 합니다.

단계

1. 응용 프로그램 * 을 선택한 다음 관리되는 응용 프로그램의 이름을 선택합니다.
2. Execution hook * 탭을 선택합니다.
3. 삭제할 후크의 경우 * Actions * 열에서 옵션 메뉴를 선택합니다.
4. 삭제 * 를 선택합니다.
5. 결과 대화 상자에 "delete"를 입력하여 확인합니다.
6. 예, 실행 후크 삭제 * 를 선택합니다.

를 참조하십시오

- "NetApp Verda GitHub 프로젝트"

Astra Control Center를 사용하여 Astra Control Center를 보호합니다

Astra Control Center가 실행 중인 Kubernetes 클러스터에서 심각한 오류로부터 복원력을 개선하려면 Astra Control Center 애플리케이션 자체를 보호합니다. 보조 Astra Control Center 인스턴스를 사용하여 Astra Control Center를 백업 및 복원하거나 기본 스토리지에서 ONTAP를 사용하는 경우 Astra 복제를 사용할 수 있습니다.

이 시나리오에서는 Astra Control Center의 두 번째 인스턴스가 다른 오류 도메인에 구축 및 구성되었으며 1차 Astra Control Center 인스턴스와 다른 두 번째 Kubernetes 클러스터에서 실행됩니다. 두 번째 Astra Control 인스턴스는 운영 Astra Control Center 인스턴스를 백업하고 복원하는 데 사용됩니다. 복원되거나 복제된 Astra Control Center 인스턴스는 애플리케이션 클러스터 애플리케이션에 대한 애플리케이션 데이터 관리를 계속 제공하며 이러한 애플리케이션의 백업 및 스냅샷에 대한 액세스 권한을 복원합니다.

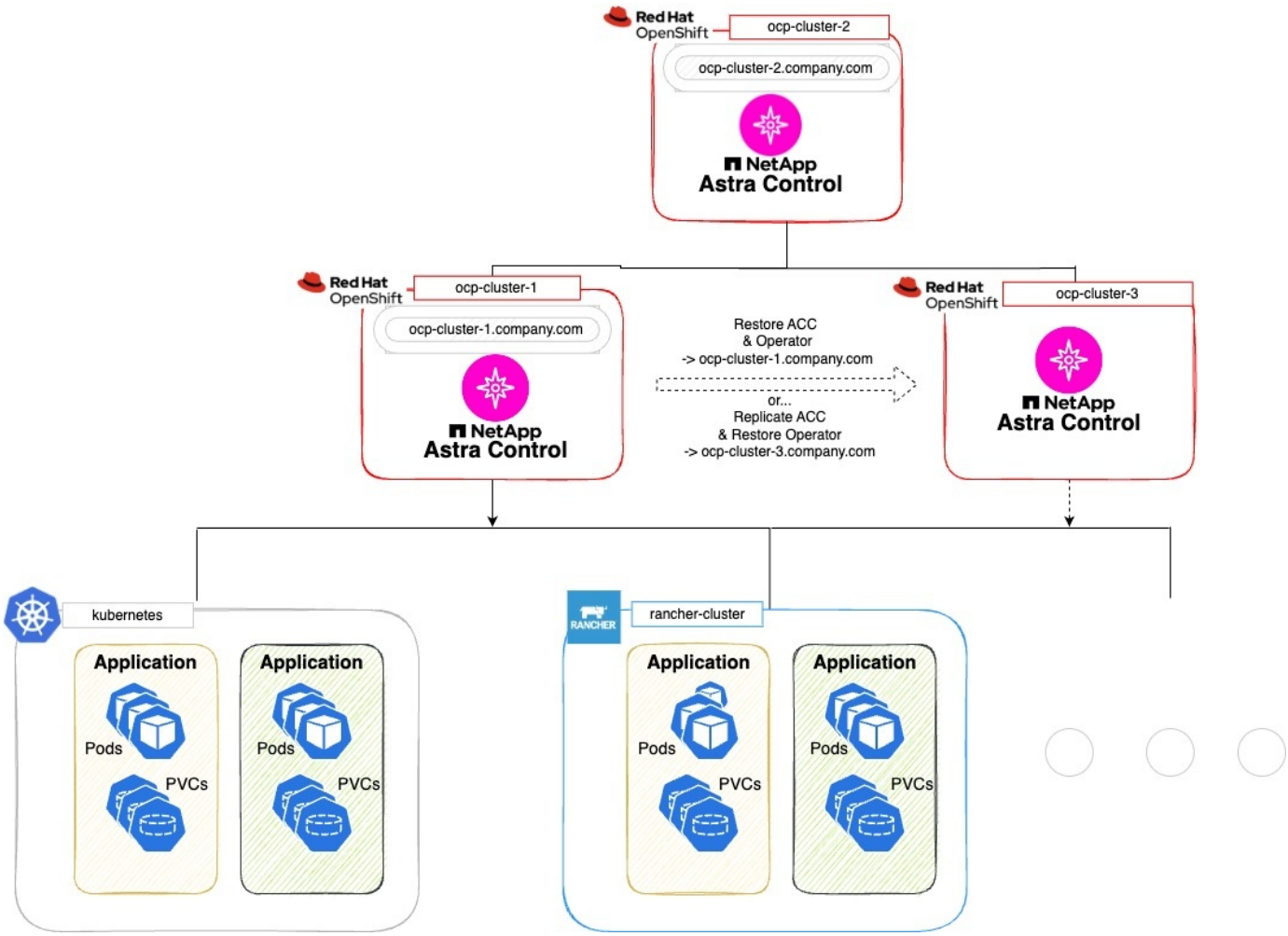
시작하기 전에

Astra Control Center에 대한 보호 시나리오를 설정하기 전에 다음 사항이 있는지 확인하십시오.

- * 1차 Astra Control Center 인스턴스를 실행하는 Kubernetes 클러스터 *: 이 클러스터는 애플리케이션 클러스터를 관리하는 1차 Astra Control Center 인스턴스를 호스팅합니다.
- * 보조 Astra Control Center 인스턴스를 실행하는 기본 시스템과 동일한 Kubernetes 배포 유형의 두 번째 Kubernetes 클러스터 *: 이 클러스터는 기본 Astra Control Center 인스턴스를 관리하는 Astra Control Center 인스턴스를 호스팅합니다.
- * 기본 Kubernetes 배포 유형이 동일한 세 번째 Kubernetes 클러스터 *: 이 클러스터는 Astra Control Center의 복원되거나 복제된 인스턴스를 호스팅합니다. 현재 운영 사이트에 구축되어 있는 것과 동일한 Astra Control Center 네임스페이스를 사용할 수 있어야 합니다. 예를 들어, Astra Control Center가 네임스페이스에 구축된 경우 `netapp-acc` 소스 클러스터에서 네임스페이스입니다 `netapp-acc` 사용 가능하고 대상 Kubernetes 클러스터의 어떤 애플리케이션에서도 사용하지 않아야 합니다.
- * S3 호환 버킷 *: 각 Astra Control Center 인스턴스에는 액세스 가능한 S3 호환 오브젝트 스토리지 버킷이 있습니다.
- * 구성된 로드 밸런서 *: 로드 밸런서는 Astra에 대한 IP 주소를 제공하며 애플리케이션 클러스터와 두 S3 버킷 모두에 대한 네트워크 연결이 있어야 합니다.
- * 클러스터가 Astra Control Center 요구 사항을 충족함 *: Astra Control Center 보호에 사용되는 각 클러스터가 충족함 "일반 Astra Control Center 요구사항".

이 작업에 대해

다음 절차에서는 다음 중 하나를 사용하여 Astra Control Center를 새 클러스터로 복원하는 데 필요한 단계를 설명합니다 백업 및 복원 또는 복제. 단계는 여기에 설명된 예제 구성을 기반으로 합니다.



이 예제 구성에서는 다음과 같이 표시됩니다.

- * 1차 Astra Control Center 인스턴스를 실행하는 Kubernetes 클러스터 *:
  - OpenShift 클러스터: `ocp-cluster-1`
  - Astra Control Center 1차 인스턴스: `ocp-cluster-1.company.com`
  - 이 클러스터는 애플리케이션 클러스터를 관리합니다.
- * 보조 Astra Control Center 인스턴스를 실행하는 기본 Kubernetes 배포 유형이 동일한 두 번째 Kubernetes 클러스터 *:
  - OpenShift 클러스터: `ocp-cluster-2`
  - Astra Control Center 2차 인스턴스: `ocp-cluster-2.company.com`
  - 이 클러스터는 기본 Astra Control Center 인스턴스를 백업하거나 다른 클러스터(이 예에서는)에 대한 복제를 구성하는 데 사용됩니다 `ocp-cluster-3` 클러스터).
- * 복원 작업에 사용될 기본 Kubernetes 배포 유형이 동일한 세 번째 Kubernetes 클러스터 *:
  - OpenShift 클러스터: `ocp-cluster-3`
  - Astra Control Center 3번째 인스턴스: `ocp-cluster-3.company.com`
  - 이 클러스터는 Astra Control Center 복원 또는 복제 페일오버에 사용됩니다.

이상적으로는, 애플리케이션 클러스터는 위의 이미지에서 Kubernetes 및 Rancher 클러스터에 설명된 대로 Astra Control Center 클러스터 3개 외부에 위치해야 합니다.

다이어그램에 표시되지 않음:

- 모든 클러스터에는 Trident가 설치된 ONTAP 백 엔드가 있습니다.
- 이 구성에서 OpenShift 클러스터는 로드 밸런서로 MetalLB를 사용합니다.
- 스냅샷 컨트롤러와 VolumeSnapshotClass도 에 설명된 대로 모든 클러스터에 설치됩니다 "필수 구성 요소".

1단계 옵션: Astra Control Center 백업 및 복원

이 절차에서는 백업 및 복원을 사용하여 Astra Control Center를 새 클러스터로 복원하는 데 필요한 단계를 설명합니다.

이 예에서는 Astra Control Center가 항상 아래에 설치됩니다 `netapp-acc` 네임스페이스 및 연산자는 아래에 설치됩니다 `netapp-acc-operator` 네임스페이스.

설명한 것은 아니지만 Astra Control Center 운영자는 Astra CR과 동일한 네임스페이스에 구축할 수도 있습니다.

시작하기 전에

- 클러스터에 운영 Astra Control Center를 설치했습니다.
- 보조 Astra Control Center를 다른 클러스터에 설치했습니다.

단계

1. 에서 실행되는 2차 Astra Control Center 인스턴스에서 운영 Astra Control Center 애플리케이션 및 타겟 클러스터를 관리합니다 `ocp-cluster-2` 클러스터):
   a. 보조 Astra Control Center 인스턴스에 로그인합니다.
   b. "1차 Astra Control Center 클러스터를 추가합니다" (`ocp-cluster-1`)를 클릭합니다.
   c. "대상 세 번째 클러스터를 추가합니다" (`ocp-cluster-3`)를 선택합니다.
2. 보조 Astra Control Center에서 Astra Control Center 및 Astra Control Center 운영자:
   a. 응용 프로그램 페이지에서 * 정의 * 를 선택합니다.
   b. Define application * (애플리케이션 정의 *) 창에서 새 애플리케이션 이름을 입력합니다 (`netapp-acc`)를 클릭합니다.
   c. 1차 Astra Control Center를 실행 중인 클러스터를 선택합니다 (`ocp-cluster-1`)를 선택합니다.
   d. 를 선택합니다 `netapp-acc` Namespace * 드롭다운 목록에서 Astra Control Center의 네임스페이스입니다.
   e. 클러스터 리소스 페이지에서 * 추가 클러스터 범위 리소스 포함 * 을 선택합니다.
   f. 포함 규칙 추가 * 를 선택합니다.
   g. 다음 항목을 선택하고 * 추가 * 를 선택합니다.
      - 라벨 선택기: <label name>
      - 그룹: apiextensions.k8s.io
      - 버전: v1

- 종류: CustomResourceDefinition

h. 응용 프로그램 정보를 확인합니다.

i. 정의 * 를 선택합니다.

정의 * 를 선택한 후 연산자에 대해 애플리케이션 정의 프로세스를 반복합니다 `netapp-acc-operator`)를 선택하고 를 선택합니다 `netapp-acc-operator` 응용 프로그램 정의 마법사의 네임스페이스입니다.

3. Astra Control Center 및 운영자 백업:

a. 보조 Astra Control Center에서 애플리케이션 탭을 선택하여 애플리케이션 페이지로 이동합니다.

b. "백업하다" Astra Control Center 애플리케이션 (`netapp-acc`)를 클릭합니다.

c. "백업하다" 오퍼레이터 (`netapp-acc-operator`)를 클릭합니다.

4. Astra Control Center와 운영자를 백업한 후 를 통해 DR(재해 복구) 시나리오를 시뮬레이션합니다 "Astra Control Center 제거 중" 운영 클러스터에서

> Astra Control Center를 새 클러스터(이 절차에서 설명하는 세 번째 Kubernetes 클러스터)에 복원하고 새로 설치된 Astra Control Center의 운영 클러스터와 동일한 DNS를 사용합니다.

5. 보조 Astra Control Center를 사용하여 "복원" Astra Control Center 애플리케이션의 1차 인스턴스:

a. 응용 프로그램 * 을 선택한 다음 Astra Control Center 응용 프로그램의 이름을 선택합니다.

b. 작업 열의 옵션 메뉴에서 * 복원 * 을 선택합니다.

c. 복원 유형으로 * Restore to new namespaces * 를 선택합니다.

d. 복원 이름을 입력합니다 (`netapp-acc`)를 클릭합니다.

e. 대상 세 번째 클러스터를 선택합니다 (`ocp-cluster-3`)를 클릭합니다.

f. 원본 네임스페이스와 동일한 네임스페이스가 되도록 대상 네임스페이스를 업데이트합니다.

g. Restore Source 페이지에서 복구 소스로 사용할 애플리케이션 백업을 선택합니다.

h. Restore using original storage classes * 를 선택합니다.

i. Restore all resources * 를 선택합니다.

j. 복원 정보를 검토한 다음 * Restore * 를 선택하여 Astra Control Center를 대상 클러스터로 복원하는 복원 프로세스를 시작합니다 (`ocp-cluster-3`)를 클릭합니다. 애플리케이션이 들어가면 복구가 완료됩니다 `available` 상태.

6. 대상 클러스터에서 Astra Control Center 구성:

a. 터미널을 열고 kubeconfig를 사용하여 대상 클러스터에 연결합니다 (`ocp-cluster-3`) 복원된 Astra Control Center가 포함되어 있습니다.

b. 를 확인합니다 `ADDRESS` Astra Control Center 구성의 열은 운영 시스템의 DNS 이름을 참조합니다.

```
kubectl get acc -n netapp-acc
```

응답:

```
NAME  UUID                                   VERSION    ADDRESS
READY
astra 89f4fd47-0cf0-4c7a-a44e-43353dc96ba8 23.10.0-68 ocp-cluster-
1.company.com           True
```

a. 를 누릅니다 `ADDRESS` 위 응답의 필드에 기본 Astra Control Center 인스턴스의 FQDN이 없습니다. Astra Control Center DNS를 참조하도록 구성을 업데이트하십시오.

```
kubectl edit acc -n netapp-acc
```

i. 를 변경합니다 `astraAddress` 에서 `spec:` FQDN으로 이동합니다 (`ocp-cluster-1.company.com` 이 예에서는 기본 Astra Control Center 인스턴스의

ii. 구성을 저장합니다.

iii. 주소가 업데이트되었는지 확인합니다.

```
kubectl get acc -n netapp-acc
```

b. 로 이동합니다 Astra Control Center Operator를 복원합니다 섹션을 참조하십시오.

1단계 옵션: 복제를 사용하여 Astra Control Center 보호

이 절차에서는 를 구성하는 데 필요한 단계를 설명합니다 "Astra Control Center 복제" 1차 Astra Control Center 인스턴스를 보호하기 위해

이 예에서는 Astra Control Center가 항상 아래에 설치됩니다 `netapp-acc` 네임스페이스 및 연산자는 아래에 설치됩니다 `netapp-acc-operator` 네임스페이스.

시작하기 전에

- 클러스터에 운영 Astra Control Center를 설치했습니다.
- 보조 Astra Control Center를 다른 클러스터에 설치했습니다.

단계

1. 보조 Astra Control Center 인스턴스에서 운영 Astra Control Center 애플리케이션 및 타겟 클러스터 관리:
   a. 보조 Astra Control Center 인스턴스에 로그인합니다.
   b. "1차 Astra Control Center 클러스터를 추가합니다" (`ocp-cluster-1`)를 클릭합니다.
   c. "대상 세 번째 클러스터를 추가합니다" (`ocp-cluster-3`)를 사용하여 복제됩니다.
2. 보조 Astra Control Center에서 Astra Control Center 및 Astra Control Center 운영자:
   a. 클러스터 * 를 선택하고 기본 Astra Control Center가 포함된 클러스터를 선택합니다 (`ocp-cluster-1`)를 클릭합니다.
   b. Namespaces* 탭을 선택합니다.

c. 를 선택합니다 `netapp-acc` 및 `netapp-acc-operator` 네임스페이스.

d. 작업 메뉴를 선택하고 * 응용 프로그램으로 정의 * 를 선택합니다.

e. 정의된 애플리케이션을 보려면 * 애플리케이션에서 보기 * 를 선택합니다.

3. 복제를 위한 백엔드 구성:

> 복제를 수행하려면 운영 Astra Control Center 클러스터와 대상 클러스터가 필요합니다 (`ocp-cluster-3`) 다른 피어링된 ONTAP 스토리지 백엔드를 사용합니다.
> 각 백엔드가 피어링되어 Astra Control에 추가되면 백엔드가 백엔드 페이지의 * 검색됨 * 탭에 표시됩니다.

a. "피어링된 백엔드를 추가합니다" 운영 클러스터의 Astra Control Center로 전환

b. "피어링된 백엔드를 추가합니다" 대상 클러스터의 Astra Control Center로 전송

4. 복제 구성:

a. Applications(응용 프로그램) 화면에서 을 선택합니다 `netapp-acc` 응용 프로그램.

b. Configure replication policy * 를 선택합니다.

c. 를 선택합니다 `ocp-cluster-3` 대상 클러스터 역할을 합니다.

d. 스토리지 클래스를 선택합니다.

e. 를 입력합니다 `netapp-acc` 대상 네임스페이스로 사용됩니다.

f. 원하는 경우 복제 빈도를 변경합니다.

g. 다음 * 을 선택합니다.

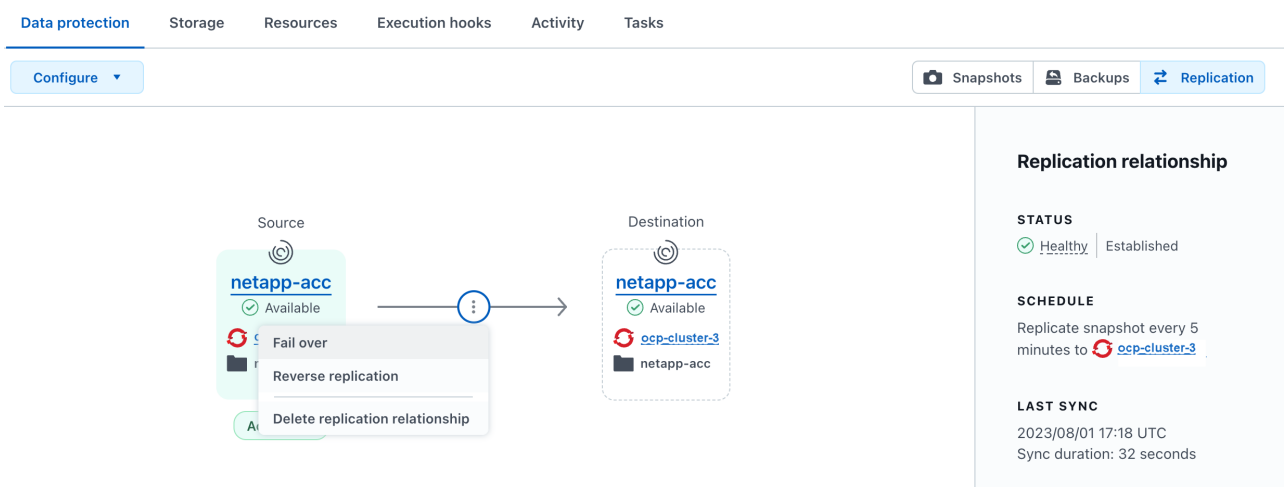
h. 구성이 올바른지 확인하고 * 저장 * 을 선택합니다.

에서 복제 관계가 전환됩니다 `Establishing` 를 선택합니다 `Established`. 활성 상태인 경우 이 복제는 복제 구성이 삭제될 때까지 5분마다 수행됩니다.

5. 운영 시스템이 손상되었거나 더 이상 액세스할 수 없는 경우 다른 클러스터로 복제를 페일오버합니다.

> 성공적인 페일오버를 보장하기 위해 대상 클러스터에 Astra Control Center가 설치되어 있지 않은지 확인합니다.

a. 수직 타원 아이콘을 선택하고 * Fail Over * 를 선택합니다.



b. 세부 정보를 확인하고 * Fail Over * 를 선택하여 페일오버 프로세스를 시작합니다.

   복제 관계 상태가 로 변경됩니다 `Failing over` 그리고 나서 `Failed over` 완료 시.

6. 페일오버 구성을 완료합니다.

   a. 터미널을 열고 세 번째 클러스터의 kubeconfig를 사용하여 연결합니다 (`ocp-cluster-3`)를 클릭합니다. 이제 이 클러스터에 Astra Control Center가 설치되었습니다.

   b. 세 번째 클러스터에서 Astra Control Center FQDN을 확인합니다 (`ocp-cluster-3`)를 클릭합니다.

   c. Astra Control Center DNS를 참조하도록 구성을 업데이트합니다.

```
kubectl edit acc -n netapp-acc
```

      i. 를 변경합니다 `astraAddress` 에서 `spec:` FQDN을 사용합니다 (`ocp-cluster-3.company.com`대상 세 번째 클러스터의).

      ii. 구성을 저장합니다.

      iii. 주소가 업데이트되었는지 확인합니다.

```
kubectl get acc -n netapp-acc
```

   d. 필요한 모든 traefik CRD가 있는지 확인합니다.

```
kubectl get crds | grep traefik
```

   필수 traefik CRD:

```
ingressroutes.traefik.containo.us
ingressroutes.traefik.io
ingressroutetcps.traefik.containo.us
ingressroutetcps.traefik.io
ingressrouteudps.traefik.containo.us
ingressrouteudps.traefik.io
middlewares.traefik.containo.us
middlewares.traefik.io
middlewaretcps.traefik.containo.us
middlewaretcps.traefik.io
serverstransports.traefik.containo.us
serverstransports.traefik.io
tlsoptions.traefik.containo.us
tlsoptions.traefik.io
tIsstores.traefik.containo.us
tIsstores.traefik.io
traefikservices.traefik.containo.us
traefikservices.traefik.io
```

a. 위의 CRD 중 일부가 누락된 경우:

i. 로 이동합니다 "Traefik 설명서".

ii. "정의" 영역을 파일로 복사합니다.

iii. 변경 내용 적용:

```
kubectl apply -f <file name>
```

iv. Traefik 다시 시작:

```
kubectl get pods -n netapp-acc | grep -e "traefik" | awk '{print
$1}' | xargs kubectl delete pod -n netapp-acc
```

b. 로 이동합니다 Astra Control Center Operator를 복원합니다 섹션을 참조하십시오.

2단계: Astra Control Center Operator를 복원합니다

보조 Astra Control Center를 사용하여 백업에서 기본 Astra Control Center 운영자를 복원합니다. 대상 네임스페이스는 소스 네임스페이스와 같아야 합니다. Astra Control Center가 운영 소스 클러스터에서 삭제된 경우에도 동일한 복원 단계를 수행하기 위한 백업은 계속 존재합니다.

단계

1. 응용 프로그램 * 을 선택한 다음 운영자 앱의 이름을 선택합니다 (`netapp-acc-operator`)를 클릭합니다.
2. 작업 열의 옵션 메뉴에서 * 복원 * 을 선택합니다

3. 복원 유형으로 * Restore to new namespaces * 를 선택합니다.
4. 대상 세 번째 클러스터를 선택합니다 (`ocp-cluster-3`)를 클릭합니다.
5. 네임스페이스를 운영 소스 클러스터에 연결된 네임스페이스와 동일하게 변경합니다 (`netapp-acc-operator`)를 클릭합니다.
6. 이전에 수행한 백업을 복구 소스로 선택합니다.
7. Restore using original storage classes * 를 선택합니다.
8. Restore all resources * 를 선택합니다.
9. 세부 정보를 검토한 후 * Restore * 를 클릭하여 복원 프로세스를 시작합니다.

   Applications 페이지에는 대상 세 번째 클러스터로 복구 중인 Astra Control Center 운영자가 표시됩니다 (`ocp-cluster-3`)를 클릭합니다. 프로세스가 완료되면 상태가 로 표시됩니다 `Available`. 10분 이내에 DNS 주소가 페이지에서 확인되어야 합니다.

결과

Astra Control Center, 등록된 클러스터, 스냅샷과 백업이 포함된 관리형 애플리케이션을 이제 타겟 세 번째 클러스터에서 사용할 수 있습니다 (`ocp-cluster-3`)를 클릭합니다. 원본에서 사용했던 보호 정책도 새 인스턴스에도 그대로 유지됩니다. 예약된 백업 또는 필요 시 백업 및 스냅샷을 계속 생성할 수 있습니다.

문제 해결

시스템 상태 및 보호 프로세스가 성공적인지 확인합니다.

- * Pod가 실행되지 않음 *: 모든 Pod가 실행 중인지 확인합니다.

  ```
  kubectl get pods -n netapp-acc
  ```

  에 일부 Pod가 있는 경우 `CrashLookBackOff` 다음과 같이 말하고 다시 시작하면 로 전환됩니다 `Running` 상태.

- * 시스템 상태 확인 *: Astra Control Center 시스템이 입력되었는지 확인합니다 `ready` 상태:

  ```
  kubectl get acc -n netapp-acc
  ```

  응답:

  ```
  NAME  UUID                                   VERSION    ADDRESS
  READY
  astra 89f4fd47-0cf0-4c7a-a44e-43353dc96ba8 23.10.0-68 ocp-cluster-
  1.company.com           True
  ```

- * 배포 상태 확인 * : Astra Control Center 배포 정보를 표시하여 이를 확인합니다 `Deployment State` 있습니다 `Deployed`.

```
kubectl describe acc astra -n netapp-acc
```

- *복원된 Astra Control Center UI가 404 오류를 반환합니다. * : 선택한 경우 이 오류가 발생합니다 `AccTraefik` 수신 옵션으로 을(를) 점검하십시오 Traefik CRD를 참조하십시오 모두 설치되었는지 확인합니다.