Astra Control Center 22.08 문서

Astra Control Center

NetApp
November 21, 2023

목차

Astra Control Center 22.08 문서

릴리스 정보

Astra Control Center의 최신 릴리스를 발표하게 되어 기쁘게 생각합니다.

- "Astra Control Center의 이번 릴리즈에는 어떤 내용이 포함되어 있는지"
- "알려진 문제"
- "Astra Data Store 및 이 Astra Control Center 릴리스와 관련된 알려진 문제입니다"
- "알려진 제한 사항"

Twitter @NetAppDoc을 팔로우하십시오. 가 되어 문서에 대한 피드백을 보냅니다 "GitHub 기고자입니다" 또는 doccomments@netapp.com 으로 이메일을 보내주십시오.

Astra Control Center의 이번 릴리스의 새로운 기능

Astra Control Center의 최신 릴리스를 발표하게 되어 기쁘게 생각합니다.

2022년 9월 8일(22.08.1)

Astra Control Center(22.08.0)용 패치 릴리스(22.08.1)는 NetApp SnapMirror를 사용하여 앱 복제에 사소한 버그를 수정합니다.

2022년 8월 10일(22.08.0)

새로운 기능 및 지원

- "NetApp SnapMirror 기술을 사용하여 애플리케이션을 복제합니다"
- "앱 관리 워크플로 개선"
- "자체 실행 후크 기능이 향상되었습니다"

> NetApp에서 제공한 특정 애플리케이션에 대한 기본 사전/사후 스냅샷 실행 후크가 이 릴리즈에서 제거되었습니다. 이 릴리즈로 업그레이드해도 스냅샷에 대한 실행 후크를 제공하지 않으면 Astra Control은 충돌 시에도 정합성이 보장되는 스냅샷만 생성합니다. 를 방문하십시오 "NetApp 버다" 사용자 환경에 맞게 수정할 수 있는 샘플 실행 후크 스크립트의 GitHub 리포지토리

- "VMware Tanzu Kubernetes Grid Integrated Edition(TKGI) 지원"
- "Google Anthos 지원"
- "LDAP 구성(Astra Control API 사용)"

알려진 문제 및 제한 사항

- "이 릴리스에 대해 알려진 문제입니다"
- "Astra Data Store 및 이 Astra Control Center 릴리스와 관련된 알려진 문제입니다"
- "이 릴리스에 대해 알려진 제한 사항입니다"

2022년 4월 26일(22.04.0)

세부 정보

새로운 기능 및 지원

- "Astra Control Center에서 Astra Data Store 배포"
- "네임스페이스 역할 기반 액세스 제어(RBAC)"
- "Cloud Volumes ONTAP 지원"
- "Astra Control Center에 대한 일반 수신 지원"
- "Astra Control에서 버킷 제거"
- "VMware Tanzu 포트폴리오 지원"

알려진 문제 및 제한 사항

- "이 릴리스에 대해 알려진 문제입니다"
- "Astra Data Store 및 이 Astra Control Center 릴리스와 관련된 알려진 문제입니다"
- "이 릴리스에 대해 알려진 제한 사항입니다"

2021년 12월 14일(21.12)

세부 정보

새로운 기능 및 지원

- "애플리케이션 복원"
- "실행 후크"
- "네임스페이스 범위 연산자로 배포된 응용 프로그램 지원"
- "업스트림 Kubernetes 및 Rancher에 대한 추가 지원"
- "Astra Data Store는 백엔드 관리 및 모니터링을 미리 봅니다"
- "Astra Control Center 업그레이드"
- "설치용 Red Hat OperatorHub 옵션"

해결된 문제

- "이 릴리스의 문제를 해결했습니다"

알려진 문제 및 제한 사항

- "이 릴리스에 대해 알려진 문제입니다"
- "Astra Data Store Preview 및 이 Astra Control Center 릴리스와 관련된 알려진 문제입니다"
- "이 릴리스에 대해 알려진 제한 사항입니다"

2021년 8월 5일(21.08)

세부 정보

Astra Control Center의 최초 릴리스.

- "그게 뭐죠"
- "아키텍처 및 구성 요소 이해"
- "시작하는 데 필요한 사항"
- "설치합니다" 및 "설정"
- "관리" 및 "보호" 인프라
- "버킷을 관리합니다" 및 "스토리지 백엔드"
- "계정 관리"
- "API를 통한 자동화"

자세한 내용을 확인하십시오

- "이 릴리스에 대해 알려진 문제입니다"
- "이 릴리스에 대해 알려진 제한 사항입니다"
- "Astra Data Store 문서"
- "이전 버전의 Astra Control Center 문서"

알려진 문제

알려진 문제점은 이 제품 릴리스를 성공적으로 사용하지 못하게 만들 수 있는 문제를 식별합니다.

현재 릴리즈에는 다음과 같은 알려진 문제가 영향을 줍니다.

인프라

- 앱 복원으로 인해 PV 크기가 원래 PV보다 큽니다
- 특정 버전의 PostgreSQL을 사용하여 앱 클론이 실패합니다
- 서비스 계정 수준 OCP SCC(Security Context Constraints)를 사용할 때 앱 클론이 실패함
- 애플리케이션 클론을 세트 스토리지 클래스로 구축한 후에는 애플리케이션 클론이 실패합니다
- 클러스터를 관리하고 볼륨을 추가한 경우 앱 백업 및 스냅숏이 실패합니다

클러스터

- 기본 kubecononfig 파일에 컨텍스트가 두 개 이상 포함되어 있으면 Astra Control Center를 사용하여 클러스터를 관리할 수 없습니다

기타 문제

- Astra Trident가 오프라인일 때 내부 서비스 오류(500)와 함께 앱 데이터 관리 작업이 실패했습니다

- 스냅샷 컨트롤러 버전 4.2.0에서 스냅숏이 실패할 수 있습니다

앱 복원으로 인해 PV 크기가 원래 PV보다 큽니다

백업을 생성한 후 영구 볼륨의 크기를 조정한 다음 해당 백업에서 복원하는 경우 영구 볼륨 크기는 백업 크기를 사용하는 대신 PV의 새 크기와 일치합니다.

특정 버전의 PostgreSQL을 사용하여 앱 클론이 실패합니다

동일한 클러스터 내의 앱 클론은 Bitnami PostgreSQL 11.5.0 차트와 함께 일관되게 실패합니다. 클론을 성공적으로 생성하려면 이전 또는 이후 버전의 차트를 사용하십시오.

서비스 계정 수준 OCP SCC(Security Context Constraints)를 사용할 때 앱 클론이 실패함

원본 보안 컨텍스트 제약 조건이 OpenShift Container Platform 클러스터의 네임스페이스 내에서 서비스 계정 수준에서 구성된 경우 애플리케이션 클론이 실패할 수 있습니다. 애플리케이션 클론이 실패하면 Astra Control Center의 Managed Applications 영역에 상태가 표시됩니다 `Removed`. 를 참조하십시오 "기술 자료 문서를 참조하십시오" 를 참조하십시오.

클러스터를 관리하고 볼륨을 추가한 경우 앱 백업 및 스냅숏이 실패합니다

와 함께 백업 및 스냅샷이 실패합니다 `UI 500 error` 이 시나리오에서. 이 문제를 해결하려면 앱 목록을 새로 고치십시오.

애플리케이션 클론을 세트 스토리지 클래스로 구축한 후에는 애플리케이션 클론이 실패합니다

스토리지 클래스가 명시적으로 설정된 상태로 응용 프로그램을 배포한 후(예: `helm install …-set global.storageClass=netapp-cvs-perf-extreme`)을 사용하여 애플리케이션을 복제하려는 이후 시도에는 타겟 클러스터에 원래 지정된 스토리지 클래스가 있어야 합니다. 명시적으로 설정된 스토리지 클래스를 가진 애플리케이션을 동일한 스토리지 클래스가 없는 클러스터로 클론 복제하면 실패합니다. 이 시나리오에서는 복구 단계가 없습니다.

기본 kubecononfig 파일에 컨텍스트가 두 개 이상 포함되어 있으면 Astra Control Center를 사용하여 클러스터를 관리할 수 없습니다

2개 이상의 클러스터와 컨텍스트를 사용하여 kubeconfig를 사용할 수 없습니다. 를 참조하십시오 "기술 자료 문서를 참조하십시오" 를 참조하십시오.

Astra Trident가 오프라인일 때 내부 서비스 오류(500)와 함께 앱 데이터 관리 작업이 실패했습니다

앱 클러스터의 Astra Trident가 오프라인 상태가 되고 다시 온라인 상태가 되고 앱 데이터 관리를 시도할 때 500 내부 서비스 오류가 발생하는 경우, 앱 클러스터의 모든 Kubernetes 노드를 다시 시작하여 기능을 복원합니다.

스냅샷 컨트롤러 버전 4.2.0에서 스냅숏이 실패할 수 있습니다

Kubernetes 1.20 또는 1.21이 포함된 Kubernetes 스냅샷 컨트롤러(외부 스냅샷 샷터라고도 함) 버전 4.2.0 을 사용하면 스냅샷이 실패할 수 있습니다. 이를 방지하려면 다른 을 사용하십시오 "지원되는 버전입니다" 4.2.1과 같은 외부 스냅샷 기능을 Kubernetes 버전 1.20 또는 1.21과 함께 사용할 수 있습니다.

1. 에 업데이트된 kubecononfig 파일을 추가하려면 POST 호출을 실행합니다 `/credentials` 지정된 을(를) 검색하고 끝점에서 가져옵니다 `id` 반응 바디에서.
2. 에서 PUT 통화를 실행합니다 `/clusters` 적절한 클러스터 ID를 사용하여 엔드포인트를 설정하고 를 설정합니다 `credentialID` 를 누릅니다 `id` 이전 단계의 값입니다.

이 단계를 완료하면 클러스터와 관련된 자격 증명이 업데이트되고 클러스터가 다시 연결되어 상태가 로 업데이트됩니다 `available`.

자세한 내용을 확인하십시오

- "Astra Data Store Preview 및 이 Astra Control Center 릴리스와 관련된 알려진 문제입니다"
- "알려진 제한 사항"

Astra Data Store 및 이 Astra Control Center 릴리스와 관련된 알려진 문제입니다

알려진 문제점은 이 제품 릴리스를 성공적으로 사용하지 못하게 만들 수 있는 문제를 식별합니다.

"이 추가 Astra Data Store 알려진 문제를 확인하십시오" 이 문제는 Astra Control Center의 현재 릴리즈와 함께 Astra Data Store의 관리에 영향을 미칠 수 있습니다.

Astra Data Store 볼륨 세부 정보는 Astra Control Center UI의 스토리지 백엔드 페이지에 나타나지 않습니다

용량 및 처리량 같은 세부 정보는 UI에 표시되지 않습니다. 이 문제가 발생하면 스토리지 백엔드의 관리를 해제하고 다시 추가합니다.

Astra Data Store로 클러스터를 관리하려면 먼저 관리되는 시스템 앱을 제거해야 합니다

Astra Data Store가 포함된 클러스터를 Astra Control Center 클러스터에 추가하면 기본적으로 Astrads-system 앱이 숨겨진 애플리케이션으로 관리됩니다. 클러스터를 관리하려면 먼저 Astrads-system 앱을 관리 해제해야 합니다. Astra Control Center UI를 사용하여 이러한 유형의 앱을 관리할 수 없습니다. 대신 Astra Control API 요청을 사용하여 앱을 수동으로 제거합니다.

세부 정보

단계

1. 이 API를 사용하여 관리되는 클러스터의 ID를 가져옵니다.

```
/accounts/{account_id}/topology/v1/managedClusters
```

응답:

```
{
"items": [
{
"type": "application/astra-managedCluster",
"version": "1.1",
"id": "123ab987-0bc0-00d0-a00a-1234567abd8d",
"name": "astrads-cluster-1234567",
...
```

2. 관리되는 Astrads 가져오기 - 시스템 앱 ID:

```
/accounts/{account_id}/topology/v2/managedClusters/{managedCluster_id}/apps
```

응답:

```
{
  "items": [
    [
      "1b011d11-bb88-40c7-a1a1-ab1234c123d3",
      "astrads-system",
      "ready"
    ]
  ],
  "metadata": {}
}
```

3. 이전 단계에서 획득한 앱 ID를 사용하여 Astads-system 앱을 삭제합니다 (`1b011d11-bb88-40c7-a1a1-ab1234c123d3`)를 클릭합니다.

```
/accounts/{account_id}/k8s/v2/apps/{astrads-system_app_id}
```

자세한 내용을 확인하십시오

- "알려진 문제"
- "알려진 제한 사항"

알려진 제한 사항

알려진 제한 사항은 이 제품 릴리스에서 지원하지 않거나 올바르게 상호 운용되지 않는 플랫폼, 장치 또는 기능을 식별합니다. 이러한 제한 사항을 주의 깊게 검토하십시오.

클러스터 관리 제한

- 두 개의 Astra Control Center 인스턴스가 동일한 클러스터를 관리할 수 없습니다
- Astra Control Center는 동일하게 이름이 지정된 두 클러스터를 관리할 수 없습니다

역할 기반 액세스 제어**(RBAC)** 제한 사항

- 네임스페이스 RBAC 제약 조건이 있는 사용자는 클러스터를 추가 및 관리할 수 있습니다
- 네임스페이스 제약 조건이 있는 구성원은 관리자가 제약 조건에 네임스페이스를 추가할 때까지 복제되거나 복원된 앱에 액세스할 수 없습니다

앱 관리 제한 사항

- pass-by-reference 연산자를 사용하여 설치된 앱의 클론이 실패할 수 있습니다
- 인증서 관리자를 사용하는 앱의 데이터 이동 없는 복원 작업은 지원되지 않습니다
- OLM 지원 및 클러스터 범위 운영자로 배포된 앱은 지원되지 않습니다
- Helm 2와 함께 배포된 앱은 지원되지 않습니다

일반 제한 사항

- Astra Control Center의 S3 버킷은 가용 용량을 보고하지 않습니다
- Astra Control Center는 프록시 서버에 대해 입력한 세부 정보를 확인하지 않습니다
- Postgres POD에 대한 기존 연결로 인해 오류가 발생합니다
- Astra Control Center 인스턴스를 제거하는 동안 백업 및 스냅샷이 보존되지 않을 수 있습니다

두 개의 **Astra Control Center** 인스턴스가 동일한 클러스터를 관리할 수 없습니다

다른 Astra Control Center 인스턴스에서 클러스터를 관리하려면 먼저 다음을 수행해야 합니다 "클러스터 관리를 취소합니다" 다른 인스턴스에서 관리하기 전에 관리되는 인스턴스에서 관리에서 클러스터를 제거한 후 다음 명령을 실행하여 클러스터가 관리되지 않는 상태인지 확인합니다.

```
oc get pods n -netapp-monitoring
```

해당 네임스페이스에서 실행 중인 포드가 없어야 합니다. 그렇지 않으면 네임스페이스가 존재하지 않아야 합니다. 둘 중 하나가 참인 경우 클러스터는 관리되지 않습니다.

Astra Control Center는 동일하게 이름이 지정된 두 클러스터를 관리할 수 없습니다

이미 있는 클러스터의 이름과 동일한 이름의 클러스터를 추가하려고 하면 작업이 실패합니다. 이 문제는 Kubernetes 구성 파일에서 클러스터 이름 기본값을 변경하지 않은 경우 표준 Kubernetes 환경에서 가장 자주 발생합니다.

해결 방법으로 다음을 수행합니다.

1. kubeadm-config ConfigMap 편집:

```
kubectl edit configmaps -n kube-system kubeadm-config
```

2. 를 변경합니다 `clusterName` 필드 값 시작 `kubernetes` 고유한 사용자 지정 이름으로 지정됩니다.
3. kubecononfig를 편집합니다 (`.kube/config`)를 클릭합니다.
4. 에서 클러스터 이름을 업데이트합니다 `kubernetes` 고유한 사용자 정의 이름으로 (`xyz-cluster` 는 아래 예제에 사용됩니다.) 두 가지 모두 업데이트합니다 `clusters` 및 `contexts` 이 예에 표시된 섹션:

```
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data:
ExAmPLERb2tCcjZ5K3E2Njk4eQotLExAMpLEORCBDRVJUSUZJQ0FURS0txxxxXX==
    server: https://x.x.x.x:6443
  name: xyz-cluster
contexts:
- context:
    cluster: xyz-cluster
    namespace: default
    user: kubernetes-admin
  name: kubernetes-admin@kubernetes
current-context: kubernetes-admin@kubernetes
```

네임스페이스 RBAC 제약 조건이 있는 사용자는 클러스터를 추가 및 관리할 수 있습니다

네임스페이스 RBAC 제약 조건이 있는 사용자는 클러스터를 추가하거나 관리할 수 없습니다. 현재 제한 사항으로 인해 Astra는 이러한 사용자가 클러스터 관리를 해제하는 것을 방지하지 않습니다.

네임스페이스 제약 조건이 있는 구성원은 관리자가 제약 조건에 네임스페이스를 추가할 때까지 복제되거나 복원된 앱에 액세스할 수 없습니다

모두 `member` 네임스페이스 이름/ID별 RBAC 제약 조건을 사용하는 사용자는 앱을 동일한 클러스터의 새 네임스페이스 또는 조직 계정의 다른 클러스터로 클론 복제 또는 복원할 수 있습니다. 그러나 동일한 사용자가 새 네임스페이스에서 복제되거나 복원된 앱에 액세스할 수 없습니다. 클론 또는 복원 작업을 통해 새 네임스페이스를 생성한 후 계정 관리자/소유자가 을 편집할 수 있습니다 `member` 영향을 받는 사용자가 새 네임스페이스에 대한 액세스 권한을 부여하도록 사용자 계정 및 역할 제약 조건을 업데이트합니다.

pass-by-reference 연산자를 사용하여 설치된 앱의 클론이 실패할 수 있습니다

Astra Control은 네임스페이스 범위 연산자와 함께 설치된 앱을 지원합니다. 이러한 연산자는 일반적으로 "pass-by-reference" 아키텍처가 아니라 "pass-by-value"로 설계되었습니다. 다음은 이러한 패턴을 따르는 일부 운영자 앱에 대한 설명입니다.

- "아파치 K8ssandra"

> K8ssandra 의 경우 현재 위치 복원 작업이 지원됩니다. 새 네임스페이스 또는 클러스터에 대한 복원 작업을 수행하려면 응용 프로그램의 원래 인스턴스를 중단해야 합니다. 이는 이월된 피어 그룹 정보가 인스턴스 간 통신으로 이어지지 않도록 하기 위한 것입니다. 앱 복제는 지원되지 않습니다.

- "젠킨스 CI"
- "Percona XtraDB 클러스터"

Astra Control은 "pass-by-reference" 아키텍처(예: CockroachDB 운영자)로 설계된 운영자를 복제하지 못할 수 있습니다. 이러한 유형의 클론 복제 작업 중에 클론 복제 운영자는 클론 복제 프로세스의 일부로 고유한 새로운 암호가 있음에도 불구하고 소스 운영자의 Kubernetes 암호를 참조하려고 합니다. Astra Control이 소스 운영자의 Kubernetes 암호를 모르기 때문에 클론 작업이 실패할 수 있습니다.

인증서 관리자를 사용하는 앱의 데이터 이동 없는 복원 작업은 지원되지 않습니다

이 Astra Control Center 릴리스는 인증서 관리자와의 응용 프로그램 데이터 이동 없는 복원을 지원하지 않습니다. 복원 작업을 다른 네임스페이스로 복원하고 클론 작업을 지원합니다.

OLM 지원 및 클러스터 범위 운영자로 배포된 앱은 지원되지 않습니다

Astra Control Center는 클러스터 범위 운영자의 애플리케이션 관리 활동을 지원하지 않습니다.

Helm 2와 함께 배포된 앱은 지원되지 않습니다

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. 자세한 내용은 을 참조하십시오 "Astra Control Center 요구 사항".

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.

Astra Control Center는 프록시 서버에 대해 입력한 세부 정보를 확인하지 않습니다

다음을 확인하십시오 "올바른 값을 입력하십시오" 연결 설정 시

Postgres POD에 대한 기존 연결로 인해 오류가 발생합니다

Postgres Pod에서 작업을 수행할 때 psql 명령을 사용하기 위해 POD 내에서 직접 연결하면 안 됩니다. Astra Control은 데이터베이스를 고정 및 고정 해제할 수 있도록 psql 액세스 권한이 필요합니다. 기존 접속이 있는 경우 스냅샷, 백업 또는 클론이 실패합니다.

Astra Control Center 인스턴스를 제거하는 동안 백업 및 스냅샷이 보존되지 않을 수 있습니다

평가 라이센스가 있는 경우 ASUP를 보내지 않을 경우 Astra Control Center에 장애가 발생할 경우 데이터 손실을 방지하기 위해 계정 ID를 저장해야 합니다.

자세한 내용을 확인하십시오

- "알려진 문제"
- "Astra Data Store 및 이 Astra Control Center 릴리스와 관련된 알려진 문제입니다"

개념

Astra Control에 대해 알아보십시오

Astra Control은 Kubernetes 애플리케이션 데이터 라이프사이클 관리 솔루션으로, 상태 저장 애플리케이션의 운영을 단순화합니다. Kubernetes 워크로드를 손쉽게 보호, 백업, 복제, 마이그레이션하고 정상 작동하는 애플리케이션 클론을 즉시 생성할 수 있습니다.

피처

Astra Control은 Kubernetes 애플리케이션 데이터 라이프사이클 관리에 중요한 기능을 제공합니다.

- 영구 스토리지를 자동으로 관리합니다
- 애플리케이션 인식 필요 시 스냅샷과 백업을 생성합니다
- 정책 기반 스냅샷 및 백업 작업 자동화
- NetApp SnapMirror 기술을 사용하여 애플리케이션을 원격 시스템에 복제합니다
- Kubernetes 클러스터 간에 애플리케이션 및 데이터를 마이그레이션합니다
- 운영 환경에서 스테이징으로 애플리케이션을 손쉽게 클론 복제할 수 있습니다
- 애플리케이션 상태 및 보호 상태를 시각화합니다
- 사용자 인터페이스 또는 API를 사용하여 백업 및 마이그레이션 워크플로우를 구현합니다

구축 모델

Astra Control은 두 가지 배포 모델로 제공됩니다.

- * Astra Control Service *: GKE(Google Kubernetes Engine) 및 AKS(Azure Kubernetes Service)에서 Kubernetes 클러스터의 애플리케이션 인식 데이터 관리를 제공하는 NetApp 관리 서비스입니다.
- * Astra Control Center *: 사내 환경에서 실행되는 Kubernetes 클러스터의 애플리케이션 인식 데이터 관리를 제공하는 자체 관리 소프트웨어입니다.

	Astra 제어 서비스	**Astra** 제어 센터
어떻게 제공됩니까**?**	NetApp에서 제공하는 완전 관리형 클라우드 서비스	소프트웨어를 다운로드, 설치 및 관리할 수 있습니다
어디에 호스팅됩니까**?**	NetApp에서 제공하는 다양한 퍼블릭 클라우드 지원	에 제공한 Kubernetes 클러스터
어떻게 업데이트됩니까**?**	NetApp에서 관리합니다	모든 업데이트를 관리합니다
애플리케이션 데이터 관리 기능은 무엇입니까**?**	스토리지 백엔드 또는 외부 서비스를 제외한 두 플랫폼에서 동일한 기능을 사용할 수 있습니다	스토리지 백엔드 또는 외부 서비스를 제외한 두 플랫폼에서 동일한 기능을 사용할 수 있습니다

	Astra 제어 서비스	**Astra** 제어 센터
스토리지 백엔드 지원이란 무엇입니까?	NetApp 클라우드 서비스 오퍼링	• NetApp ONTAP AFF 및 FAS 시스템 • 스토리지 백엔드로 Astra Data Store를 사용합니다 • Cloud Volumes ONTAP 스토리지 백엔드

Astra Control Service의 작동 방식

Astra Control Service는 NetApp에서 관리하는 클라우드 서비스로, 항상 최신 기능을 사용하여 업데이트 가능합니다. 이 솔루션은 여러 구성 요소를 활용하여 애플리케이션 데이터 수명 주기 관리를 지원합니다.

높은 수준에서 Astra Control Service는 다음과 같이 작동합니다.

- 클라우드 공급자를 설정하고 Astra 계정에 등록하여 Astra Control Service를 시작할 수 있습니다.
  - GKE 클러스터의 경우 Astra Control Service가 사용합니다 "Google Cloud용 NetApp Cloud Volumes Service" 또는 Google 영구 디스크를 영구 볼륨의 스토리지 백엔드로 사용합니다.
  - AKS 클러스터의 경우 Astra Control Service가 사용합니다 "Azure NetApp Files" 또는 Azure Disk Storage를 영구 볼륨의 스토리지 백엔드로 사용합니다.
  - Amazon EKS 클러스터의 경우 Astra Control Service가 사용합니다 "Amazon Elastic Block Store를 클릭합니다" 또는 "NetApp ONTAP용 Amazon FSx" 영구 볼륨의 스토리지 백엔드로 사용됩니다.
- 첫 번째 Kubernetes 컴퓨팅을 Astra Control Service에 추가합니다. 그러면 Astra Control Service에서 다음을 수행합니다.
  - 클라우드 공급자 계정에 백업 복사본이 저장되는 개체 저장소를 만듭니다.

    Azure에서 Astra Control Service는 Blob 컨테이너용 리소스 그룹, 스토리지 계정 및 키도 생성합니다.
  - 클러스터에 새 관리 역할 및 Kubernetes 서비스 계정을 생성합니다.
  - 에서는 새 관리자 역할을 사용하여 를 설치합니다 "아스트라 트리덴트" 를 클릭하여 하나 이상의 스토리지 클래스를 생성합니다.
  - Azure NetApp Files 또는 NetApp Cloud Volumes Service for Google Cloud를 스토리지 백엔드로 사용하는 경우, Astra Control Service는 Astra Trident를 사용하여 앱에 영구 볼륨을 프로비저닝합니다.
- 이제 앱을 클러스터에 추가할 수 있습니다. 영구 볼륨은 새로운 기본 스토리지 클래스에 프로비저닝됩니다.
- 그런 다음 Astra Control Service를 사용하여 이러한 애플리케이션을 관리하고 스냅샷, 백업 및 클론 생성을 시작합니다.

Astra Control의 무료 플랜을 사용하면 최대 10개의 앱을 계정에서 관리할 수 있습니다. 10개 이상의 앱을 관리하려면 무료 요금에서 프리미엄 요금제로 업그레이드하여 청구서를 설정해야 합니다.

Astra Control Center의 작동 방식

Astra Control Center는 프라이빗 클라우드에서 로컬로 실행됩니다.

Astra Control Center는 다음과 같은 기능을 통해 Kubernetes 클러스터를 지원합니다.

- ONTAP 9.5 이상의 Trident 스토리지 백엔드
- Astra Data Store 스토리지 백엔드

클라우드 연결 환경에서 Astra Control Center는 Cloud Insights를 사용하여 고급 모니터링 및 원격 측정 기능을 제공합니다. Cloud Insights 연결이 없을 경우 Astra Control Center에서 제한된(7일 메트릭) 모니터링 및 원격 측정 기능을 사용할 수 있으며, 개방형 메트릭 엔드 포인트를 통해 Kubernetes 기본 모니터링 툴(예: Prometheus 및 Grafana)으로 내보낼 수 있습니다.

Astra Control Center는 AutoSupport 및 Active IQ 에코시스템에 완전히 통합되어 사용자와 NetApp 지원에 문제 해결 및 사용 정보를 제공합니다.

90일 평가판 라이센스를 사용하여 Astra Control Center를 사용해 볼 수 있습니다. 평가 버전은 이메일 및 커뮤니티(Slack 채널) 옵션을 통해 지원됩니다. 또한 제품 내 지원 대시보드에서 Knowledgebase 문서 및 문서에 액세스할 수 있습니다.

Astra Control Center를 설치하고 사용하려면 반드시 충족해야 합니다 "요구 사항".

Astra Control Center는 다음과 같이 높은 수준에서 작동합니다.

- 현지 환경에 Astra Control Center를 설치합니다. 에 대해 자세히 알아보십시오 "Astra Control Center를 설치합니다".
- 다음과 같은 몇 가지 설정 작업을 완료합니다.
  - 라이센스를 설정합니다.
  - 첫 번째 클러스터를 추가합니다.
  - 클러스터를 추가할 때 검색된 스토리지 백엔드를 추가합니다.
  - 앱 백업을 저장할 오브젝트 저장소 버킷을 추가합니다.

에 대해 자세히 알아보십시오 "Astra Control Center를 설정합니다".

Astra Control Center는 다음과 같은 작업을 수행합니다.

- 네임스페이스를 비롯하여 클러스터에 대한 세부 정보를 검색하고 앱을 정의 및 보호할 수 있습니다.
- 관리하려는 클러스터에서 Astra Trident 또는 Astra Data Store 구성을 검색하고 스토리지 백엔드를 모니터링할 수 있습니다.

앱을 클러스터에 추가할 수 있습니다. 클러스터에 이미 관리 중인 앱이 있으면 Astra Control Center를 사용하여 관리할 수 있습니다. 그런 다음 Astra Control Center를 사용하여 스냅샷, 백업, 클론 및 복제 관계를 생성합니다.

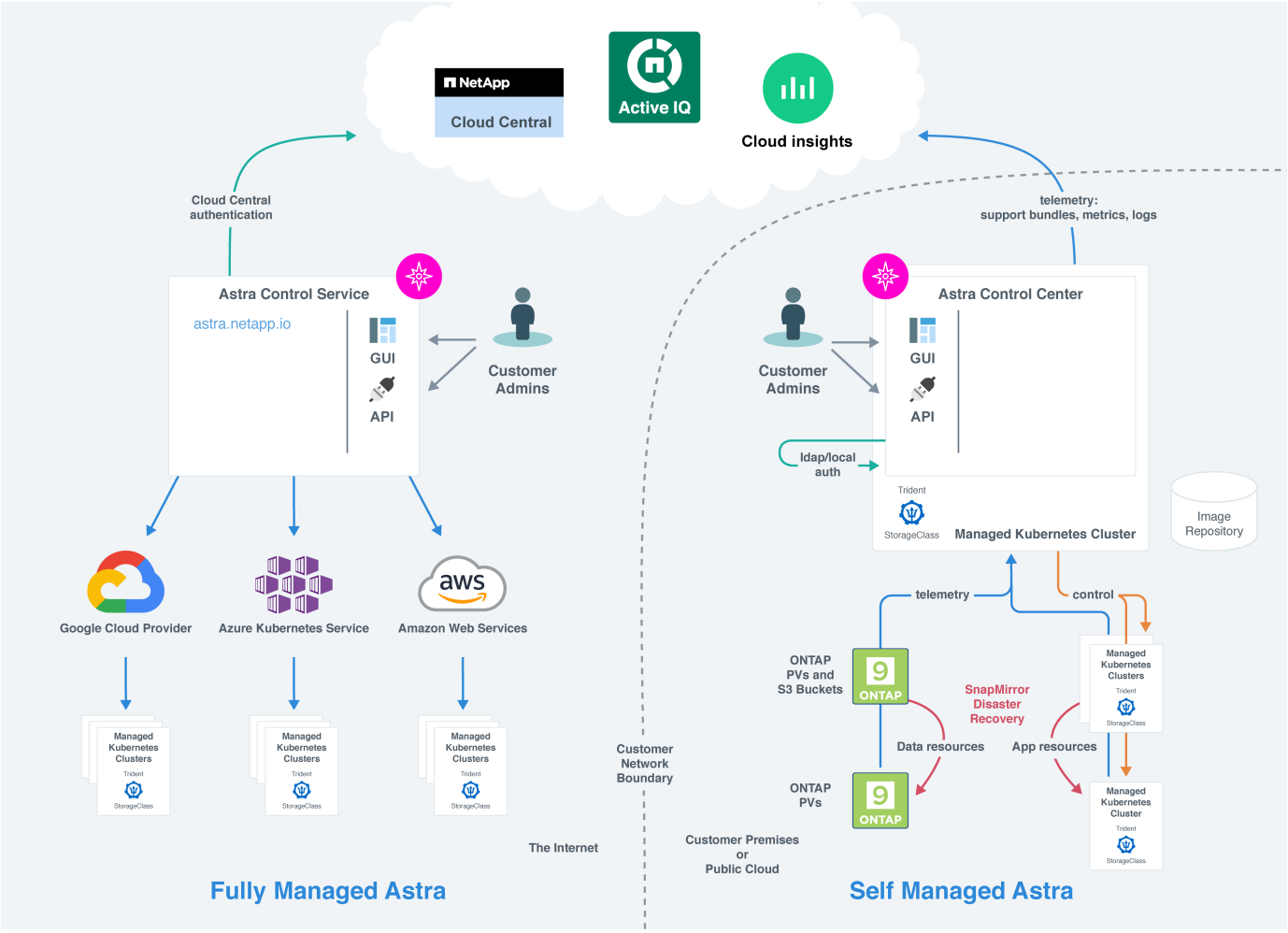
를 참조하십시오

- "Astra Control Service 문서"
- "Astra Control Center 문서"
- "Astra Data Store 문서"
- "Astra Trident 문서"
- "Astra Control API를 사용합니다"
- "Cloud Insights 설명서"

- "ONTAP 설명서"

아키텍처 및 구성 요소

이 슬라이드에는 Astra Control 환경의 다양한 구성 요소에 대한 개요가 나와 있습니다.



Astra Control 구성 요소

- * Kubernetes 클러스터 *: Kubernetes는 컨테이너식 워크로드 및 서비스를 관리할 수 있는 확장 가능한 휴대용 오픈 소스 플랫폼으로, 선언적 구성과 자동화를 모두 지원합니다. Astra는 Kubernetes 클러스터에서 호스팅되는 애플리케이션에 관리 서비스를 제공합니다.
- * Astra Trident *: NetApp에서 관리하며 완벽한 지원을 제공하는 오픈 소스 스토리지 공급자 및 오케스트레이터로서, Trident는 Docker 및 Kubernetes에서 관리하는 컨테이너식 애플리케이션용 스토리지 볼륨을 생성할 수 있도록 지원합니다. Astra Control Center와 함께 구축한 경우, Trident는 구성된 ONTAP 스토리지 백엔드를 포함합니다.
- * 스토리지 백엔드 *:
  - Astra Control Service는 다음과 같은 스토리지 백엔드를 사용합니다.
    - "Google Cloud용 NetApp Cloud Volumes Service" 또는 GKE 클러스터의 스토리지 백엔드로 Google 영구 디스크를 사용할 수 있습니다
    - "Azure NetApp Files" 또는 Azure 관리 디스크를 AKS 클러스터의 스토리지 백엔드로 사용합니다.

        - "Amazon EBS(Elastic Block Store)" 또는 "NetApp ONTAP용 Amazon FSx" EKS 클러스터에 대한 백엔드 스토리지 옵션으로 제공됩니다.
    - Astra Control Center는 다음과 같은 스토리지 백엔드를 사용합니다.
        - ONTAP AFF and FAS를 참조하십시오. 스토리지 소프트웨어 및 하드웨어 플랫폼인 ONTAP는 핵심 스토리지 서비스, 다중 스토리지 액세스 프로토콜 지원 및 스냅샷, 미러링과 같은 스토리지 관리 기능을 제공합니다.
        - Cloud Volumes ONTAP
- * Cloud Insights *: NetApp 클라우드 인프라 모니터링 툴인 Cloud Insights를 사용하면 Astra Control Center에서 관리하는 Kubernetes 클러스터의 성능과 활용률을 모니터링할 수 있습니다. Cloud Insights는 스토리지 사용량과 워크로드를 상호 연관시킵니다. Astra Control Center에서 Cloud Insights 연결을 활성화하면 Astra Control Center UI 페이지에 원격 측정 정보가 표시됩니다.

Astra Control 인터페이스

다른 인터페이스를 사용하여 작업을 완료할 수 있습니다.

- * 웹 UI(사용자 인터페이스) *: Astra Control Service와 Astra Control Center는 동일한 웹 기반 UI를 사용하여 앱을 관리, 마이그레이션 및 보호할 수 있습니다. UI를 사용하여 사용자 계정 및 구성 설정을 관리할 수도 있습니다.
- * API *: Astra Control Service와 Astra Control Center는 동일한 Astra Control API를 사용합니다. API를 사용하면 UI를 사용할 때와 동일한 작업을 수행할 수 있습니다.

또한 Astra Control Center를 사용하면 VM 환경 내에서 실행 중인 Kubernetes 클러스터를 관리, 마이그레이션 및 보호할 수 있습니다.

를 참조하십시오

- "Astra Control Service 문서"
- "Astra Control Center 문서"
- "Astra Trident 문서"
- "Astra Control API를 사용합니다"
- "Cloud Insights 설명서"
- "ONTAP 설명서"

데이터 보호

Astra Control Center에서 사용 가능한 데이터 보호 유형과 이를 사용하여 앱을 보호하는 최선의 방법에 대해 알아보십시오.

스냅샷, 백업 및 보호 정책

snapshot_은 앱과 동일한 프로비저닝된 볼륨에 저장된 앱의 시점 복사본입니다. 대개 빠릅니다. 로컬 스냅샷을 사용하여 애플리케이션을 이전 시점으로 복원할 수 있습니다. 스냅샷은 빠른 클론에 유용합니다. 스냅샷에는 구성 파일을 포함하여 앱의 모든 Kubernetes 객체가 포함됩니다.

백업 _ 은(는) 외부 오브젝트 저장소에 저장되며 로컬 스냅샷과 비교하여 더 느리게 실행할 수 있습니다. 앱 백업을 동일한 클러스터에 복원하거나 백업을 다른 클러스터에 복원하여 앱을 마이그레이션할 수 있습니다. 또한 백업의 보존

기간을 더 길게 선택할 수도 있습니다. 이러한 백업은 외부 개체 저장소에 저장되므로 일반적으로 서버 장애 또는 데이터 손실 시 스냅샷보다 더 뛰어난 보호 기능을 제공합니다.

보호 정책 _ 은(는) 해당 앱에 대해 정의한 일정에 따라 스냅샷, 백업 또는 둘 모두를 자동으로 생성하여 앱을 보호하는 방법입니다. 또한 보호 정책을 통해 일정에 유지할 스냅샷 및 백업의 수를 선택할 수 있습니다. 보호 정책을 통해 백업 및 스냅샷을 자동화하는 것이 조직의 요구에 따라 각 앱을 보호하는 가장 좋은 방법입니다.

> _최근 백업 _ 이(가) 있을 때까지 완전히 보호할 수 없습니다. 백업은 영구 볼륨으로부터 멀리 떨어진 개체 저장소에 저장되기 때문에 이 작업이 중요합니다. 장애 또는 사고로 인해 클러스터와 관련 영구 스토리지가 삭제되면 복구할 백업이 필요합니다. 스냅샷을 사용하면 복구할 수 없습니다.

복제

clone_은 앱, 해당 구성 및 영구 스토리지의 정확한 복제입니다. 동일한 Kubernetes 클러스터 또는 다른 클러스터에 클론을 수동으로 생성할 수 있습니다. 애플리케이션 및 스토리지를 Kubernetes 클러스터 간에 이동해야 하는 경우 앱 클론을 생성하는 것이 유용할 수 있습니다.

원격 클러스터에 복제

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 클러스터 간에 데이터 및 애플리케이션 변경사항을 복제할 수 있습니다.

Astra Control은 애플리케이션 스냅샷 복사본을 원격 클러스터에 비동기식으로 복제합니다. 복제 프로세스에는 SnapMirror에 의해 복제된 영구 볼륨의 데이터와 Astra Control에 의해 보호되는 애플리케이션 메타데이터가 포함됩니다.

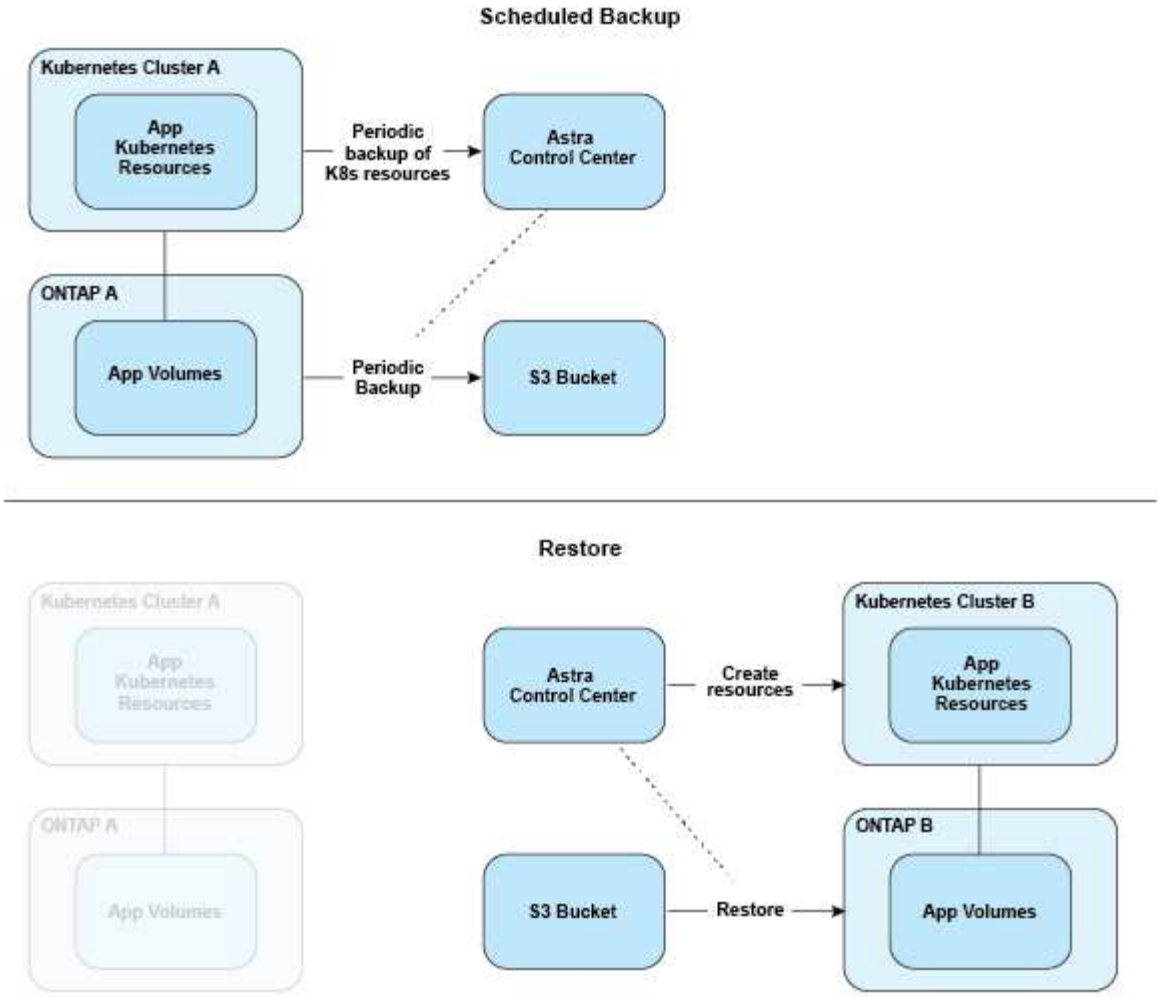
앱 복제는 다음과 같은 방식으로 앱 백업 및 복원과 다릅니다.

- * 앱 복제 *: Astra Control을 사용하려면 NetApp SnapMirror를 지원하도록 구성된 각 ONTAP 스토리지 백엔드를 통해 소스 및 대상 Kubernetes 클러스터를 사용하고 관리해야 합니다. Astra Control은 정책 기반 애플리케이션 스냅샷을 생성하여 원격 클러스터에 복제합니다. NetApp SnapMirror 기술은 영구 볼륨 데이터를 복제하는 데 사용됩니다. Astra Control은 페일오버하기 위해 대상 Kubernetes 클러스터의 앱 객체를 대상 ONTAP 클러스터의 복제된 볼륨으로 재생성하여 복제된 앱을 온라인으로 전환할 수 있습니다. 대상 ONTAP 클러스터에 영구 볼륨 데이터가 이미 있으므로 Astra Control은 페일오버에 대한 빠른 복구 시간을 제공할 수 있습니다.
- * 애플리케이션 백업 및 복원 *: 애플리케이션을 백업할 때 Astra Control은 애플리케이션 데이터의 스냅샷을 생성하고 이를 오브젝트 스토리지 버킷에 저장합니다. 복원이 필요한 경우 버킷 내의 데이터를 ONTAP 클러스터의 영구 볼륨에 복사해야 합니다. 백업/복원 작업에서는 보조 Kubernetes/ONTAP 클러스터를 사용하고 관리할 필요가 없지만, 추가 데이터 복사본을 사용할 경우 복원 시간이 길어질 수 있습니다.

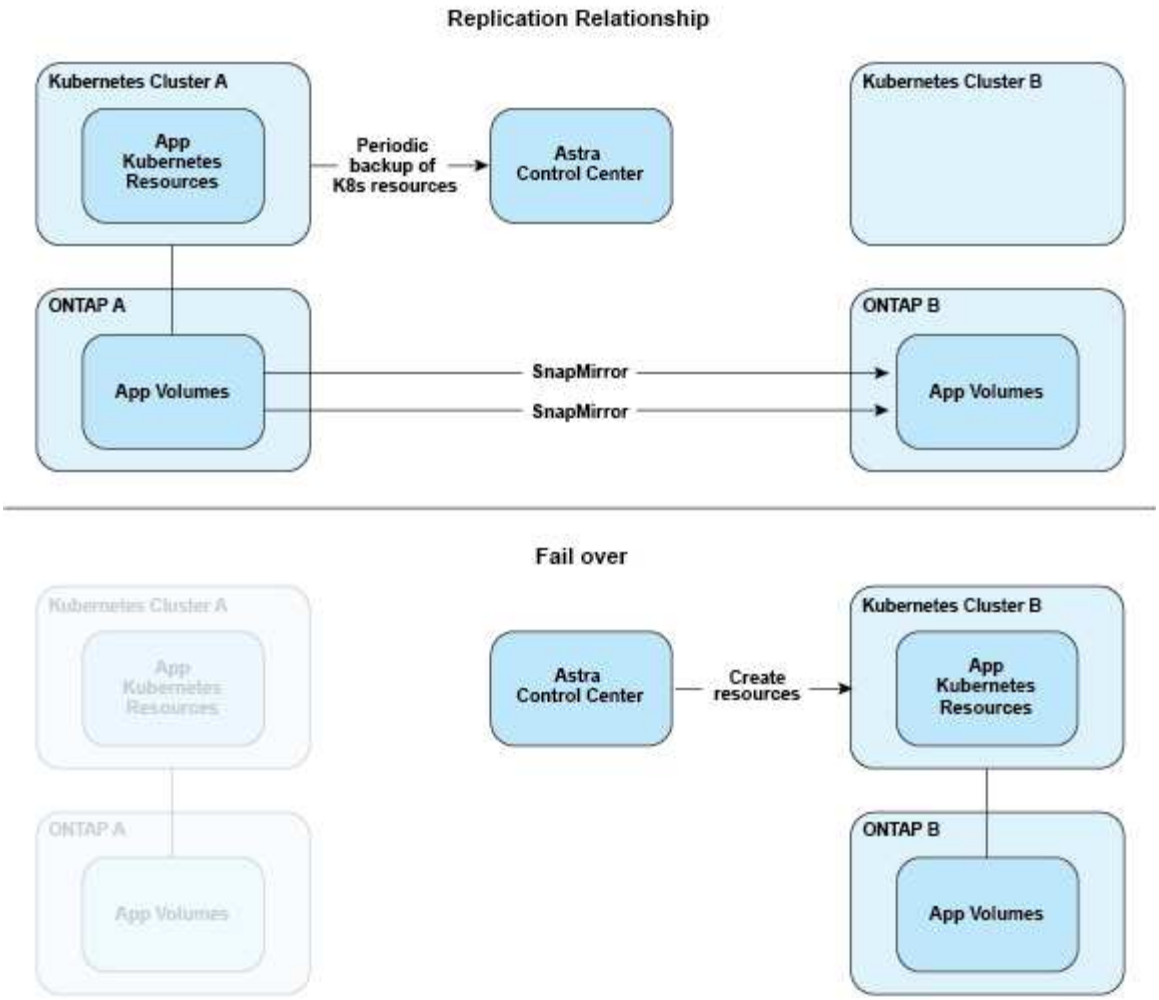
앱을 복제하는 방법에 대한 자세한 내용은 을 참조하십시오 "SnapMirror 기술을 사용하여 원격 시스템에 애플리케이션을 복제합니다".

다음 이미지는 복제 프로세스와 비교하여 예약된 백업 및 복원 프로세스를 보여 줍니다.

백업 프로세스는 데이터를 S3 버킷으로 복사하고 S3 버킷에서 복원:



반면, 복제는 ONTAP로 복제하여 수행하지만 페일오버로 Kubernetes 리소스를 생성합니다.



라이센싱

Astra Control Center는 전체 앱 데이터 관리 기능을 사용하려면 라이센스를 설치해야 합니다. 라이센스 없이 Astra Control Center를 배포하는 경우, 시스템 기능이 제한된다는 경고 메시지가 웹 UI에 표시됩니다.

애플리케이션과 데이터를 보호하려면 라이센스가 필요합니다. Astra Control Center를 참조하십시오 "피처" 를 참조하십시오.

제품 구입 후 제품 번호와 라이센스가 제공됩니다. 에서 NetApp 라이센스 파일(NLF)을 생성할 수 있습니다 "NetApp Support 사이트".

또한 평가판 라이센스가 있는 Astra Control Center를 사용하여 라이센스를 다운로드한 날짜로부터 90일 동안 Astra Control Center를 사용할 수 있습니다. 자세한 내용은 을 참조하십시오 "요구 사항".

ONTAP 스토리지 백엔드에 필요한 라이센스에 대한 자세한 내용은 을 참조하십시오 "지원되는 스토리지 백엔드".

ⓘ 라이센스 없이 클러스터를 추가하고, 버킷을 추가하고, 스토리지 백엔드를 관리할 수 있습니다.

라이선스 소비량의 계산 방법

Astra Control Center에 새 클러스터를 추가하면 클러스터에서 실행 중인 하나 이상의 애플리케이션이 Astra Control Center에 의해 관리되기 전에는 사용된 라이센스에 포함되지 않습니다.

클러스터에서 응용 프로그램 관리를 시작하면 해당 클러스터의 모든 CPU 장치가 Astra Control Center 라이센스 소모에 포함됩니다.

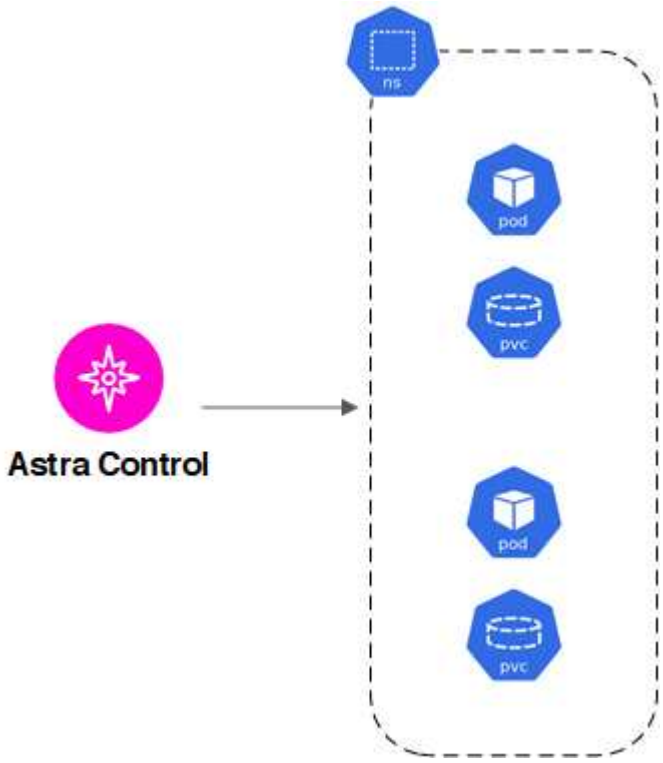
자세한 내용을 확인하십시오

- "기존 라이센스를 업데이트합니다"

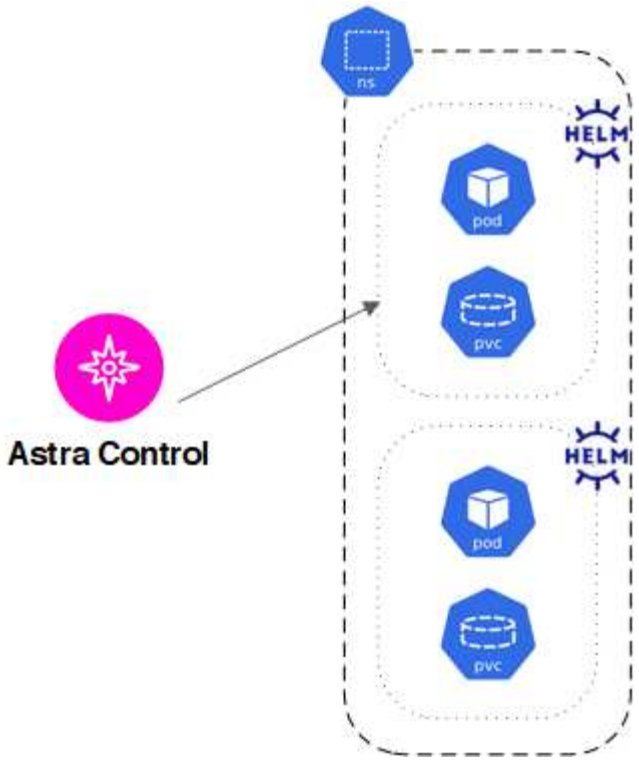
앱 관리 이해

Astra Control이 클러스터를 검색할 때 해당 클러스터의 앱은 관리 방법을 선택할 때까지 관리되지 않습니다. Astra Control에서 관리되는 응용 프로그램은 다음 중 하나일 수 있습니다.

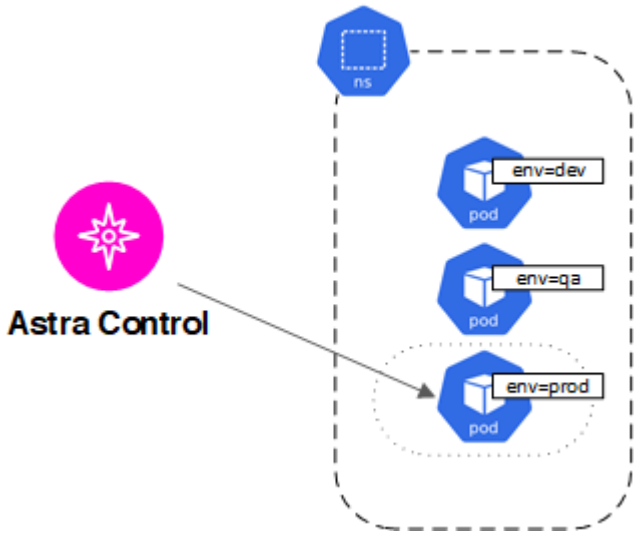
- 네임스페이스에서 모든 리소스를 포함하는 네임스페이스입니다



- 네임스페이스 내에 배포된 개별 애플리케이션(이 예에서는 helm3이 사용됨)



- 네임스페이스 내의 Kubernetes 레이블로 식별되는 리소스 그룹입니다



스토리지 클래스 및 영구 볼륨 크기

Astra Control Center는 스토리지 백엔드로 ONTAP 또는 Astra Data Store를 지원합니다.

개요

Astra Control Center는 다음을 지원합니다.

- * Astra Data Store 스토리지에서 지원하는 Trident 스토리지 클래스 *: 하나 이상의 Astra Data Store 클러스터를 수동으로 설치한 경우, Astra Control Center는 이러한 클러스터를 가져오고 토폴로지(노드, 디스크)와 다양한 상태를 검색할 수 있는 기능을 제공합니다.

Astra Control Center는 Astra Data Store 구성의 기본 Kubernetes 클러스터, Kubernetes 클러스터가 속한 클라우드, Astra Data Store에서 프로비저닝한 영구 볼륨, 해당 내부 볼륨의 이름, 영구 볼륨을 사용하는 애플리케이션, 앱이 포함된 클러스터를 표시합니다.

- * ONTAP 스토리지에서 지원하는 Trident 스토리지 클래스 *: ONTAP 백엔드를 사용하는 경우, Astra 제어 센터에서 ONTAP 백엔드를 가져와 다양한 모니터링 정보를 보고할 수 있습니다.

> Trident 스토리지 클래스는 Astra Control Center 외부에서 사전 구성되어 있어야 합니다.

스토리지 클래스

Astra Control Center에 클러스터를 추가하면 해당 클러스터에서 이전에 구성된 스토리지 클래스 중 하나를 기본 스토리지 클래스로 선택하라는 메시지가 표시됩니다. 이 스토리지 클래스는 영구 볼륨 클레임(PVC)에 지정된 저장소 클래스가 없을 때 사용됩니다. 기본 스토리지 클래스는 Astra Control Center 내에서 언제든지 변경할 수 있으며, PVC 또는 H제어 차트 내에서 스토리지 클래스의 이름을 지정하여 언제든지 모든 스토리지 클래스를 사용할 수 있습니다. Kubernetes 클러스터에 대해 단일 기본 스토리지 클래스만 정의되어 있는지 확인하십시오.

Astra Data Store 스토리지 백엔드와 통합된 Astra Control Center를 사용하는 경우 설치 후 스토리지 클래스가 정의되지 않습니다. Trident 기본 스토리지 클래스를 생성하여 스토리지 백엔드에 적용해야 합니다. 을 참조하십시오 "Astra Data Store를 시작하는 중입니다" 기본 Astra Data Store 스토리지 클래스를 생성합니다.

를 참조하십시오

- "Astra Trident 문서"

사용자 역할 및 네임스페이스

Astra Control의 사용자 역할 및 네임스페이스, 그리고 이를 사용하여 조직의 리소스에 대한 액세스를 제어하는 방법에 대해 알아봅니다.

사용자 역할

역할을 사용하여 Astra Control의 리소스 또는 기능에 대한 사용자의 액세스를 제어할 수 있습니다. Astra Control의 사용자 역할은 다음과 같습니다.

- Viewer * 는 리소스를 볼 수 있습니다.
- 구성원 * 은 뷰어 역할 권한을 가지며 앱 및 클러스터를 관리하고, 앱을 관리하고, 스냅샷 및 백업을 삭제할 수 있습니다.
- Admin * 은 구성원 역할 권한을 가지며 소유자를 제외한 다른 사용자를 추가 및 제거할 수 있습니다.
- 소유자 * 는 관리자 역할 권한을 가지며 모든 사용자 계정을 추가 및 제거할 수 있습니다.

멤버 또는 뷰어 사용자에게 제약 조건을 추가하여 사용자를 하나 이상의 사용자로 제한할 수 있습니다 [네임스페이스].

네임스페이스

네임스페이스는 Astra Control에서 관리하는 클러스터 내의 특정 리소스에 할당할 수 있는 범위입니다. Astra Control은 클러스터를 Astra Control에 추가할 때 클러스터의 네임스페이스를 검색합니다. 네임스페이스가 검색되면 사용자에게 제약 조건으로 할당할 수 있습니다. 해당 네임스페이스에 대한 액세스 권한이 있는 멤버만 해당 리소스를 사용할 수 있습니다. 회사 내의 물리적 영역이나 부서 등 조직에 적합한 패러다임을 사용하여 네임스페이스에 대한 액세스를

제어할 수 있습니다. 사용자에게 제약 조건을 추가하면 해당 사용자가 모든 네임스페이스에 액세스하거나 특정 네임스페이스 집합만 액세스하도록 구성할 수 있습니다. 네임스페이스 레이블을 사용하여 네임스페이스 제약 조건을 할당할 수도 있습니다.

자세한 내용을 확인하십시오

"역할을 관리합니다"

시작하십시오

Astra Control Center 요구 사항

먼저 운영 환경, 애플리케이션 클러스터, 애플리케이션, 라이센스 및 웹 브라우저의 준비 상태를 확인하십시오.

- 구현할 수 있습니다
- 지원되는 스토리지 백엔드
- 애플리케이션 클러스터 요구사항
- [설명합니다]
- 복제 사전 요구 사항
- 인터넷 접속
- [라이센스]
- 온프레미스 Kubernetes 클러스터의 수신
- 네트워킹 요구 사항
- 지원되는 웹 브라우저

구현할 수 있습니다

Astra Control Center는 다음과 같은 유형의 운영 환경에서 검증되었습니다.

- Google Anthos 1.10 또는 1.11
- Kubernetes 1.22 ~ 1.24
- RKE(Rancher Kubernetes Engine):
  - RKE 1.2.16 w/Rancher 2.5.12 및 RKE 1.3.3 w/2.6.3
  - RKE 2 (v1.23.6 + rke2r2), Rancher 2.6.3
- Red Hat OpenShift Container Platform 4.8, 4.9 또는 4.10
- VMware Tanzu Kubernetes Grid 1.4 또는 1.5
- VMware Tanzu Kubernetes Grid Integrated Edition 1.12.2 또는 1.13

Astra Control Center를 호스팅하기 위해 선택한 운영 환경이 환경 공식 문서에 설명된 기본 리소스 요구 사항을 충족하는지 확인합니다. Astra Control Center에는 환경의 리소스 요구 사항 외에 다음과 같은 리소스가 필요합니다.

구성 요소	요구 사항
스토리지 백엔드 용량입니다	최소 500GB가 제공됩니다
작업자 노드	최소 3개의 작업자 노드, 각각 4개의 CPU 코어, 12GB RAM
FQDN 주소입니다	Astra Control Center의 FQDN 주소입니다

구성 요소	요구 사항
아스트라 트리덴트	Astra Trident 21.10.1 이상 SnapMirror 기반 애플리케이션 복제를 위해 Astra Trident 22.07 이상 설치 및 구성되었습니다

이러한 요구 사항에서는 Astra Control Center가 운영 환경에서 실행되는 유일한 애플리케이션이라고 가정합니다. 환경에서 추가 애플리케이션이 실행 중인 경우 이러한 최소 요구 사항을 적절히 조정합니다.

- * 이미지 레지스트리 *: Astra Control Center 빌드 이미지를 푸시할 수 있는 기존 개인 Docker 이미지 레지스트리가 있어야 합니다. 이미지를 업로드할 이미지 레지스트리의 URL을 제공해야 합니다.
- * Astra Trident/ONTAP 구성 *: Astra Control Center를 사용하려면 스토리지 클래스를 생성하고 기본 스토리지 클래스로 설정해야 합니다. Astra Control Center는 Astra Trident에서 제공하는 다음과 같은 ONTAP 드라이버를 지원합니다.
  - ONTAP - NAS
  - ONTAP-SAN
  - ONTAP-SAN - 경제성

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`

두 번째 OpenShift 운영 환경을 관리되는 컴퓨팅 리소스로 추가할 계획이라면 Astra Trident Volume Snapshot 기능이 활성화되어 있는지 확인해야 합니다. Astra Trident를 사용하여 볼륨 스냅샷을 활성화하고 테스트하려면 "공식 Astra Trident 지침을 참조하십시오".

VMware Tanzu Kubernetes Grid 클러스터 요구 사항

VMware Tanzu Kubernetes Grid(TKG) 또는 Tanzu Kubernetes Grid Integrated Edition(TKGi) 클러스터에서 Astra Control Center를 호스팅하는 경우 다음 사항을 고려하십시오.

- Astra Control에서 관리하려는 모든 애플리케이션 클러스터에서 TKG 또는 TKGi 기본 스토리지 클래스 적용을 비활성화합니다. 를 편집하여 이 작업을 수행할 수 있습니다 `TanzuKubernetesCluster` 리소스 를 확인하십시오.
- Astra Control Center 설치의 일부로 POD 보안 정책(PSP) 제한 환경에서 다음 리소스가 생성됩니다.
  - POD 보안 정책
  - RBAC 역할
  - RBAC RoleBinding RBAC 역할 및 RoleBinding 리소스가 에 만들어집니다 `netapp-acc` 네임스페이스.
- TKG 또는 TKGi 환경에 Astra Control Center를 구축하는 경우 Astra Trident에 대한 특정 요구 사항을 숙지하십시오. 자세한 내용은 를 참조하십시오 "Astra Trident 문서".

> 기본 VMware TKG 및 TKGi 구성 파일 토큰은 구축 후 10시간 후에 만료됩니다. Tanzu 포트폴리오 제품을 사용하는 경우, Astra Control Center와 관리되는 애플리케이션 클러스터 간의 연결 문제를 방지하기 위해 만료되지 않는 토큰이 포함된 Tanzu Kubernetes Cluster 구성 파일을 생성해야 합니다. 자세한 내용은 를 참조하십시오 "VMware NSX-T 데이터 센터 제품 설명서"

Google Anthos 클러스터 요구 사항

Google Anthos 클러스터에서 Astra Control Center를 호스팅할 때 Google Anthos에는 기본적으로 MetalLB 로드 밸런서와 Istio 수신 게이트웨이 서비스가 포함되어 있으므로 설치 중에 Astra Control Center의 일반적인 수신 기능을 사용할 수 있습니다. 을 참조하십시오 "Astra Control Center를 구성합니다" 를 참조하십시오.

지원되는 스토리지 백엔드

Astra Control Center는 다음과 같은 스토리지 백엔드를 지원합니다.

- NetApp ONTAP 9.5 이상 AFF 및 FAS 시스템
- NetApp ONTAP 9.8 이상 SnapMirror 기반 애플리케이션 복제를 위한 AFF 및 FAS 시스템
- NetApp Cloud Volumes ONTAP를 참조하십시오

Astra Control Center를 사용하려면 수행해야 할 작업에 따라 다음과 같은 ONTAP 라이센스가 있는지 확인합니다.

- 플랙스클론
- SnapMirror: 선택 사항. SnapMirror 기술을 사용하여 원격 시스템에 복제하는 경우에만 필요합니다. 을 참조하십시오 "SnapMirror 라이센스 정보".
- S3 라이센스: 선택 사항. ONTAP S3 버킷에만 필요

ONTAP 시스템에 필요한 라이센스가 있는지 확인할 수 있습니다. 을 참조하십시오 "ONTAP 라이센스 관리".

애플리케이션 클러스터 요구사항

Astra Control Center에는 Astra Control Center에서 관리하려는 클러스터에 대한 다음과 같은 요구 사항이 있습니다. 이러한 요구 사항은 관리하려는 클러스터가 Astra Control Center를 호스팅하는 운영 환경 클러스터인 경우에도 적용됩니다.

- Kubernetes의 최신 버전입니다 "스냅샷 컨트롤러 구성 요소입니다" 이(가) 설치되었습니다
- Astra Trident "볼륨스냅샷 클래스 개체" 관리자가 정의했습니다
- 클러스터에 기본 Kubernetes 스토리지 클래스가 있습니다
- Astra Trident를 사용하도록 스토리지 클래스를 하나 이상 구성했습니다

> 애플리케이션 클러스터에는 가 있어야 합니다 `kubeconfig.yaml` 한 _CONTEXT_ELEMENT만 정의하는 파일입니다. 에 대한 Kubernetes 설명서를 참조하십시오 "kubecononfig 파일 생성에 대한 정보입니다".

> Rancher 환경에서 애플리케이션 클러스터를 관리할 때 에서 애플리케이션 클러스터의 기본 컨텍스트를 수정합니다 `kubeconfig` Rancher API 서버 컨텍스트 대신 컨트롤 플레인 컨텍스트를 사용하기 위해 Rancher에서 제공하는 파일입니다. 따라서 Rancher API 서버의 부하가 줄어들고 성능이 향상됩니다.

설명합니다

Astra Control에는 다음과 같은 애플리케이션 관리 요구 사항이 있습니다.

- * 라이선스 *: Astra Control Center를 사용하여 애플리케이션을 관리하려면 Astra Control Center 라이센스가 필요합니다.
- * Namespaces *: Astra Control은 앱이 단일 네임스페이스 이상의 범위를 포괄하지 않도록 하지만 네임스페이스에는 여러 개의 앱이 포함될 수 있습니다.
- * StorageClass *: StorageClass가 명시적으로 설정된 애플리케이션을 설치하고 앱을 복제해야 하는 경우 클론 작업의 타겟 클러스터에 원래 지정된 StorageClass가 있어야 합니다. 명시적으로 StorageClass를 동일한 StorageClass가 없는 클러스터로 설정한 애플리케이션을 클론 복제하면 실패합니다.
- * Kubernetes 리소스 *: Astra Control에서 수집하지 않은 Kubernetes 리소스를 사용하는 애플리케이션에는 전체 앱 데이터 관리 기능이 없을 수 있습니다. Astra Control은 다음과 같은 Kubernetes 리소스를 수집합니다.

클러스터 역할	ClusterRoleBinding 을 참조하십시오	ConfigMap을 클릭합니다
경작업	사용자 지정 리소스 정의	CustomResource 를 선택합니다
DemonSet	DeploymentConfig(배포 구성	HorizontalPodAutoscaler
침투	뮤atingWebhook	네트워크 정책
PersistentVolumeClaim	포드	팟캐스트 예산
팟캐스트 템플릿	ReplicaSet입니다	역할
RoleBinding 을 클릭합니다	루트	비밀
서비스	서비스 계정	StatefulSet 을 선택합니다
Webhook을 확인합니다		

복제 사전 요구 사항

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

- 원활한 재해 복구를 위해 세 번째 장애 도메인 또는 보조 사이트에 Astra Control Center를 배포하는 것이 좋습니다.
- 앱의 호스트 Kubernetes 클러스터 및 대상 Kubernetes 클러스터를 사용할 수 있고 서로 다른 장애 도메인 또는 사이트에서 이상적인 두 ONTAP 클러스터에 연결할 수 있어야 합니다.
- ONTAP 클러스터와 호스트 SVM이 페어링되어야 합니다. 을 참조하십시오 "클러스터 및 SVM 피어링 개요".
- 타겟 클러스터의 Trident에서 페어링된 원격 SVM을 사용할 수 있어야 합니다.
- Trident 버전 22.07 이상이 소스 및 대상 ONTAP 클러스터 모두에 있어야 합니다.
- 소스 및 대상 ONTAP 클러스터 모두에서 데이터 보호 번들을 사용하는 ONTAP SnapMirror 비동기식 라이센스를 설정해야 합니다. 을 참조하십시오 "ONTAP의 SnapMirror 라이센스 개요".
- ONTAP 스토리지 백엔드를 Astra 제어 센터에 추가할 때 액세스 방법이 있는 "admin" 역할을 사용하여 사용자 자격 증명을 적용합니다 `http` 및 `ontapi` 두 ONTAP 클러스터에서 모두 활성화 을 참조하십시오 "사용자 계정 관리" 를 참조하십시오.
- 소스 및 대상 Kubernetes 클러스터와 ONTAP 클러스터는 Astra Control에서 관리해야 합니다.

> 다른 클러스터 또는 사이트에서 실행 중인 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.

자세한 내용을 알아보십시오 "SnapMirror 기술을 사용하여 원격 시스템에 애플리케이션을 복제합니다".

지원되는 응용 프로그램 설치 방법

Astra Control은 다음과 같은 응용 프로그램 설치 방법을 지원합니다.

- * 매니페스트 파일 *: Astra Control은 kubctl을 사용하여 매니페스트 파일에서 설치된 앱을 지원합니다. 예를 들면 다음과 같습니다.

  ```
  kubectl apply -f myapp.yaml
  ```

- * Helm 3 *: Helm을 사용하여 앱을 설치하는 경우 Astra Control에 Helm 버전 3이 필요합니다. Helm 3(또는 Helm 2에서 Helm 3으로 업그레이드)과 함께 설치된 앱의 관리 및 클론 생성이 완벽하게 지원됩니다. Helm 2가 설치된 앱 관리는 지원되지 않습니다.
- * 운용자 구축 앱 *: Astra Control은 네임스페이스 범위 연산자와 함께 설치된 앱을 지원합니다. 다음은 이 설치 모델에 대해 검증된 몇 가지 응용 프로그램들입니다.
  - "아파치 K8ssandra"
  - "젠킨스 CI"
  - "Percona XtraDB 클러스터"

> 운영자와 설치하는 앱은 동일한 네임스페이스를 사용해야 합니다. 운영자가 배포 .YAML 파일을 수정해야 할 수도 있습니다.

인터넷 접속

인터넷에 대한 외부 액세스 권한이 있는지 확인해야 합니다. 그렇지 않으면 NetApp Cloud Insights에서 모니터링 및 메트릭 데이터를 수신하거나 지원 번들을 보내는 등 일부 기능이 제한될 수 있습니다 "NetApp Support 사이트".

라이센스

Astra Control Center의 모든 기능을 사용하려면 Astra Control Center 라이센스가 필요합니다. NetApp에서 평가판 라이센스 또는 전체 라이센스를 받으십시오. 애플리케이션과 데이터를 보호하려면 라이센스가 필요합니다. 을 참조하십시오 "Astra Control Center의 특징" 를 참조하십시오.

Astra Control Center에 평가판 라이센스를 사용하면 라이센스를 다운로드한 날짜로부터 90일 동안 Astra Control Center를 사용할 수 있습니다. 등록하면 무료 평가판을 사용할 수 있습니다 "여기".

ONTAP 스토리지 백엔드에 필요한 라이센스에 대한 자세한 내용은 을 참조하십시오 "지원되는 스토리지 백엔드".

라이센스 작동 방법에 대한 자세한 내용은 을 참조하십시오 "라이센싱".

온프레미스 **Kubernetes** 클러스터의 수신

네트워크 수신 Astra Control Center 사용 유형을 선택할 수 있습니다. 기본적으로 Astra Control Center는 클러스터 차원의 리소스로 Astra Control Center 게이트웨이(서비스/traefik)를 배포합니다. 또한 Astra Control Center는 서비스 로드 밸런서가 사용자 환경에서 허용되는 경우 이를 사용할 수 있도록 지원합니다. 서비스 로드 밸런서를 사용하고 아직 서비스 로드 밸런서가 구성되어 있지 않은 경우 MetalLB 로드 밸런서를 사용하여 외부 IP 주소를 서비스에 자동으로 할당할 수 있습니다. 내부 DNS 서버 구성에서 Astra Control Center에 대해 선택한 DNS 이름을 부하 분산 IP 주소로 지정해야 합니다.

> Tanzu Kubernetes Grid 클러스터에 Astra Control Center를 호스팅하는 경우 를 사용하십시오 `kubectl get nsxlbmonitors -A` 수신 트래픽을 허용하도록 서비스 모니터가 이미 구성되어 있는지 확인하는 명령입니다. 기존 서비스 모니터가 새 로드 밸런서 구성을 무시하므로 MetalLB를 설치하면 안 됩니다.

자세한 내용은 을 참조하십시오 "부하 분산을 위한 수신 설정".

네트워킹 요구 사항

Astra Control Center를 호스팅하는 운영 환경은 다음 TCP 포트를 사용하여 통신합니다. 이러한 포트가 모든 방화벽을 통해 허용되는지 확인하고 Astra 네트워크에서 발생하는 HTTPS 송신 트래픽을 허용하도록 방화벽을 구성해야 합니다. 일부 포트에는 Astra Control Center를 호스팅하는 환경과 각 관리 클러스터(해당되는 경우) 간의 연결이 모두 필요합니다.

> Astra Control Center를 이중 스택 Kubernetes 클러스터에 구축할 수 있으며, Astra Control Center는 이중 스택 작업을 위해 구성된 애플리케이션 및 스토리지 백엔드를 관리할 수 있습니다. 이중 스택 클러스터 요구사항에 대한 자세한 내용은 를 참조하십시오 "Kubernetes 문서".

출처	목적지	포트	프로토콜	목적
클라이언트 PC	Astra 제어 센터	443	HTTPS	UI/API 액세스 - Astra Control Center를 호스팅하는 클러스터와 관리되는 각 클러스터 간에 이 포트가 열려 있는지 확인합니다
소비자 평가 기준	Astra Control Center 작업자 노드	9090	HTTPS	메트릭 데이터 통신 - 각 관리 클러스터가 Astra Control Center를 호스팅하는 클러스터의 이 포트에 액세스할 수 있는지 확인합니다 (양방향 통신 필요)
Astra 제어 센터	Hosted Cloud Insights 서비스	443	HTTPS	Cloud Insights 통신
Astra 제어 센터	Amazon S3 스토리지 버킷 공급자	443	HTTPS	Amazon S3 스토리지 통신

출처	목적지	포트	프로토콜	목적
Astra 제어 센터	NetApp AutoSupport를 참조하십시오	443	HTTPS	NetApp AutoSupport 커뮤니케이션

지원되는 웹 브라우저

Astra Control Center는 1280 x 720의 최소 해상도로 최신 버전의 Firefox, Safari 및 Chrome을 지원합니다.

다음 단계

를 봅니다 "빠른 시작" 개요.

Astra Control Center를 빠르게 시작합니다

이 페이지에서는 Astra Control Center를 시작하는 데 필요한 단계에 대해 개괄적으로 설명합니다. 각 단계의 링크를 클릭하면 자세한 내용을 제공하는 페이지로 이동합니다.

사용해 보세요! Astra Control Center를 사용해 보고 싶은 경우 90일 평가판 라이센스를 사용할 수 있습니다. 을 참조하십시오 "라이센스 정보" 를 참조하십시오.

1 **Kubernetes** 클러스터 요구사항을 검토하십시오

- Astra는 Trident에서 구성한 ONTAP 스토리지 백엔드 또는 Astra Data Store 스토리지 백엔드를 통해 Kubernetes 클러스터와 함께 작동합니다.
- 클러스터는 정상 상태에서 실행되어야 하며 3개 이상의 온라인 작업자 노드가 있어야 합니다.
- 클러스터가 Kubernetes를 실행 중이어야 합니다.

에 대해 자세히 알아보십시오 "Astra Control Center 요구 사항".

2 **Astra Control Center**를 다운로드하여 설치합니다

- 에서 Astra Control Center를 다운로드합니다 "NetApp Support 사이트 Astra Control Center 다운로드 페이지".
- 현지 환경에 Astra Control Center를 설치합니다.

  필요한 경우 Red Hat OperatorHub를 사용하여 Astra Control Center를 설치합니다.

  필요한 경우 Cloud Volumes ONTAP 스토리지 백엔드를 사용하여 Astra Control Center를 설치합니다.

에 대해 자세히 알아보십시오 "Astra Control Center 설치".

3 몇 가지 초기 설정 작업을 완료합니다

- Astra Control 라이센스와 지원 ONTAP 라이센스를 추가합니다.
- Kubernetes 클러스터 추가 및 Astra Control Center에서 세부 정보를 검색합니다.

- ONTAP 스토리지 백엔드를 추가합니다.
- 필요에 따라 앱 백업을 저장할 오브젝트 저장소 버킷을 추가합니다.

에 대해 자세히 알아보십시오 "초기 설정 프로세스".

4 **Astra Control Center**를 사용합니다

Astra Control Center 설정을 마치면 다음 단계를 수행하십시오.

- 앱을 관리합니다. 에 대해 자세히 알아보십시오 "앱 관리".
- 앱에 대한 보호 정책을 구성하고, 앱을 원격 시스템으로 복제하고, 앱을 복제 및 마이그레이션하여 앱을 보호합니다. 에 대해 자세히 알아보십시오 "앱 보호".
- 계정 관리(사용자, 역할, 사용자 인증을 위한 LDAP, 자격 증명, 리포지토리 연결 등) 에 대해 자세히 알아보십시오 "사용자 관리".
- 필요한 경우 NetApp Cloud Insights에 연결하여 Astra Control Center UI 내에서 시스템 상태, 용량 및 처리량에 대한 메트릭을 표시할 수 있습니다. 에 대해 자세히 알아보십시오 "Cloud Insights에 연결 중입니다".

5 이 빠른 시작에서 계속합니다

"Astra Control Center를 설치합니다".

자세한 내용을 확인하십시오

- "Astra Control API를 사용합니다"

설치 개요

다음 Astra Control Center 설치 절차 중 하나를 선택하여 완료합니다.

- "표준 프로세스를 사용하여 Astra Control Center를 설치합니다"
- "(Red Hat OpenShift를 사용하는 경우) OpenShift OperatorHub를 사용하여 Astra Control Center를 설치합니다"
- "Cloud Volumes ONTAP 스토리지 백엔드를 사용하여 Astra Control Center를 설치합니다"

표준 프로세스를 사용하여 **Astra Control Center**를 설치합니다

Astra Control Center를 설치하려면 NetApp Support 사이트에서 설치 번들을 다운로드하고 다음 단계를 수행하여 해당 환경에 Astra Control Center Operator and Astra Control Center를 설치합니다. 이 절차를 사용하여 인터넷에 연결되었거나 공기가 연결된 환경에 Astra Control Center를 설치할 수 있습니다.

Red Hat OpenShift 환경에서는 을 사용할 수 있습니다 "대체 절차" OpenShift OperatorHub를 사용하여 Astra Control Center를 설치하려면 다음을 수행합니다.

필요한 것

- "설치를 시작하기 전에 Astra Control Center 구축을 위한 환경을 준비합니다".

- 사용자 환경에서 POD 보안 정책을 구성했거나 구성하려는 경우 POD 보안 정책 및 해당 정책이 Astra Control Center 설치에 어떤 영향을 미치는지 숙지하십시오. 을 참조하십시오 "POD 보안 정책 제한 사항 이해".
- 모든 클러스터 운영자가 양호한 상태이며 사용 가능한지 확인합니다.

```
kubectl get clusteroperators
```

- 모든 API 서비스가 정상 상태이며 사용 가능한지 확인합니다.

```
kubectl get apiservices
```

- 사용하려는 Astra FQDN이 이 클러스터에 라우팅될 수 있는지 확인합니다. 즉, 내부 DNS 서버에 DNS 항목이 있거나 이미 등록된 코어 URL 경로를 사용하고 있는 것입니다.
- 클러스터에 인증서 관리자가 이미 있는 경우 일부를 수행해야 합니다 "필수 단계" 따라서 Astra Control Center는 자체 인증 관리자를 설치하지 않습니다.

이 작업에 대해

Astra Control Center 설치 프로세스는 다음을 수행합니다.

- 에 Astra 구성 요소를 설치합니다 `netapp-acc` (또는 사용자 지정 이름) 네임스페이스입니다.
- 기본 계정을 만듭니다.
- 기본 관리 사용자 이메일 주소와 기본 1회 암호를 설정합니다. 이 사용자에게는 시스템에서 UI에 처음 로그인하는 데 필요한 소유자 역할이 할당됩니다.
- 모든 Astra Control Center Pod가 실행 중인지 확인하는 데 도움이 됩니다.
- Astra UI를 설치합니다.

> (Astra Data Store Early Access Program(EAP) 릴리즈에만 적용) Astra Control Center를 사용하여 Astra Data Store를 관리하고 VMware 워크플로우를 활성화하려면 에 Astra Control Center만 배포하십시오 `pcloud` 에 없는 네임스페이스입니다 `netapp-acc` 네임스페이스 또는 사용자 지정 네임스페이스는 이 절차의 단계에 설명되어 있습니다.

> 모든 Astra Control Center Pod를 삭제하지 않도록 설치 프로세스 내내 다음 명령을 실행하지 마십시오. `kubectl delete -f astra_control_center_operator_deploy.yaml`

> Docker Engine 대신 Red Hat의 Podman 명령을 사용하는 경우 Docker 명령 대신 Podman 명령을 사용할 수 있습니다.

단계

Astra Control Center를 설치하려면 다음 단계를 수행하십시오.

- Astra Control Center 번들을 다운로드하고 포장을 풉니다
- NetApp Astra kubtl 플러그인을 설치합니다
- 이미지를 로컬 레지스트리에 추가합니다

- 인증 요구 사항이 있는 레지스트리에 대한 네임스페이스 및 암호를 설정합니다
- Astra Control Center 운영자를 설치합니다
- Astra Control Center를 구성합니다
- Astra 제어 센터 및 운전자 설치를 완료합니다
- 시스템 상태를 확인합니다
- 부하 분산을 위한 수신 설정
- Astra Control Center UI에 로그인합니다

Astra Control Center 번들을 다운로드하고 포장을 풉니다

1. Astra Control Center 번들을 다운로드합니다 (`astra-control-center-[version].tar.gz`)를 선택합니다 "NetApp Support 사이트".
2. 에서 Astra Control Center 인증서 및 키의 지퍼를 다운로드합니다 "NetApp Support 사이트".
3. (선택 사항) 다음 명령을 사용하여 번들의 서명을 확인합니다.

```
openssl dgst -sha256 -verify AstraControlCenter-public.pub -signature
astra-control-center-[version].tar.gz.sig astra-control-center-
[version].tar.gz
```

4. 이미지 추출:

```
tar -vxzf astra-control-center-[version].tar.gz
```

NetApp Astra kubtl 플러그인을 설치합니다

NetApp 아스트라 `kubectl` 명령줄 플러그인을 사용하면 Astra Control Center 배포 및 업그레이드와 관련된 일반적인 작업을 수행할 때 시간을 절약할 수 있습니다.

필요한 것

NetApp은 다양한 CPU 아키텍처 및 운영 체제용 플러그인의 바이너리를 제공합니다. 이 작업을 수행하기 전에 사용 중인 CPU 및 운영 체제를 알아야 합니다. Linux 및 Mac 운영 체제에서는 를 사용할 수 있습니다 `uname -a` 명령을 사용하여 이 정보를 수집합니다.

단계

1. 사용 가능한 NetApp Astra를 나열하십시오 `kubectl` 플러그인 바이너리를 만들고 운영 체제 및 CPU 아키텍처에 필요한 파일 이름을 적어 둡니다.

```
ls kubectl-astra/
```

2. 파일을 규격과 같은 위치에 복사합니다 `kubectl` 유틸리티. 이 예에서 는 입니다 `kubectl` 유틸리티는 에 있습니다 `/usr/local/bin` 디렉토리. 대치 `<binary-name>` 필요한 파일 이름:

```
cp kubectl-astra/<binary-name> /usr/local/bin/kubectl-astra
```

이미지를 로컬 레지스트리에 추가합니다

1. 용기 엔진에 적합한 단계 시퀀스를 완료합니다.

Docker 를 참조하십시오

1. Astra 디렉토리로 이동합니다.

```
cd acc
```

2. Astra Control Center 이미지 디렉토리에 있는 패키지 이미지를 로컬 레지스트리로 푸시합니다. 명령을 실행하기 전에 다음 대체 작업을 수행합니다.
   - Bundle_file을 Astra Control 번들 파일 이름으로 바꿉니다(예: `acc.manifest.yaml`)를 클릭합니다.
   - my_registry를 Docker 리포지토리의 URL로 바꿉니다.
   - my_registry_user를 사용자 이름으로 바꿉니다.
   - my_registry_token을 레지스트리에 대한 인증된 토큰으로 바꿉니다.

```
kubectl astra packages push-images -m BUNDLE_FILE -r MY_REGISTRY
-u MY_REGISTRY_USER -p MY_REGISTRY_TOKEN
```

팟맨

1. 레지스트리에 로그인합니다.

```
podman login [your_registry_path]
```

2. 설명에 명시된 대로 <your_registry> 대체를 만들어 다음 스크립트를 실행합니다.

```
# You need to be at the root of the tarball.
# You should see these files to confirm correct location:
#   acc.manifest.yaml
#   acc/

# Replace <YOUR_REGISTRY> with your own registry (e.g
registry.customer.com or registry.customer.com/testing, etc..)
export REGISTRY=<YOUR_REGISTRY>
export PACKAGENAME=acc
export PACKAGEVERSION=22.08.1-26
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
  # Load to local cache
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')

  # Remove path and keep imageName.
  astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')

  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/netapp/astra/${PACKAGENAME}
/${PACKAGEVERSION}/${astraImageNoPath}

  # Push to the local repo.
  podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done
```

인증 요구 사항이 있는 레지스트리에 대한 네임스페이스 및 암호를 설정합니다

1. Astra Control Center 호스트 클러스터에 대한 KUBECONFIG를 내보냅니다.

```
export KUBECONFIG=[file path]
```

2. 인증이 필요한 레지스트리를 사용하는 경우 다음을 수행해야 합니다.

   a. 를 생성합니다 `netapp-acc-operator` 네임스페이스:

```
kubectl create ns netapp-acc-operator
```

   응답:

```
namespace/netapp-acc-operator created
```

b. 에 대한 암호를 만듭니다 `netapp-acc-operator` 네임스페이스. Docker 정보를 추가하고 다음 명령을 실행합니다.

> 자리 표시자입니다 `your_registry_path` 이전에 업로드한 이미지의 위치와 일치해야 합니다(예: `[Registry_URL]/netapp/astra/astracc/22.08.1-26`)를 클릭합니다.

```
kubectl create secret docker-registry astra-registry-cred -n netapp-
acc-operator --docker-server=[your_registry_path] --docker-username
=[username] --docker-password=[token]
```

샘플 반응:

```
secret/astra-registry-cred created
```

> 암호를 생성한 후 네임스페이스를 삭제하는 경우 네임스페이스를 다시 만든 후 네임스페이스에 대한 암호를 다시 생성해야 합니다.

c. 를 생성합니다 `netapp-acc` (또는 사용자 지정 이름) 네임스페이스입니다.

```
kubectl create ns [netapp-acc or custom namespace]
```

샘플 반응:

```
namespace/netapp-acc created
```

d. 에 대한 암호를 만듭니다 `netapp-acc` (또는 사용자 지정 이름) 네임스페이스입니다. Docker 정보를 추가하고 다음 명령을 실행합니다.

```
kubectl create secret docker-registry astra-registry-cred -n [netapp-
acc or custom namespace] --docker-server=[your_registry_path]
--docker-username=[username] --docker-password=[token]
```

응답

```
secret/astra-registry-cred created
```

a. [[substep_kubecononfig_secret] (선택 사항) 설치 후 Astra Control Center에서 클러스터를 자동으로

관리하려는 경우 이 명령을 사용하여 배포할 Astra Control Center 네임스페이스 내에서 kubecononfig를 암호로 제공해야 합니다.

```
kubectl create secret generic [acc-kubeconfig-cred or custom secret name] --from-file=<path-to-your-kubeconfig> -n [netapp-acc or custom namespace]
```

Astra Control Center 운영자를 설치합니다

1. 디렉토리를 변경합니다.

```
cd manifests
```

2. Astra Control Center 운영자 배포 YAML을 편집합니다 (`astra_control_center_operator_deploy.yaml`)를 클릭하여 로컬 레지스트리 및 암호를 참조합니다.

```
vim astra_control_center_operator_deploy.yaml
```

> YAML 주석이 붙은 샘플은 다음 단계를 따릅니다.

a. 인증이 필요한 레지스트리를 사용하는 경우 의 기본 줄을 바꿉니다 `imagePullSecrets: []` 다음 포함:

```
imagePullSecrets:
- name: <astra-registry-cred>
```

b. 변경 `[your_registry_path]` 의 경우 `kube-rbac-proxy` 이미지를 에서 푸시한 레지스트리 경로로 이미지 이전 단계.

c. 변경 `[your_registry_path]` 의 경우 `acc-operator-controller-manager` 이미지를 에서 푸시한 레지스트리 경로로 이미지 이전 단계.

d. (Astra Data Store Preview를 사용하여 설치하는 경우) 와 관련된 알려진 문제를 참조하십시오 "스토리지 클래스 프로비저닝 및 YAML에 대한 추가 변경 사항".

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
  name: acc-operator-controller-manager
  namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
      containers:
      - args:
        - --secure-listen-address=0.0.0.0:8443
        - --upstream=http://127.0.0.1:8080/
        - --logtostderr=true
        - --v=10
        image: [your_registry_path]/kube-rbac-proxy:v4.8.0
        name: kube-rbac-proxy
        ports:
        - containerPort: 8443
          name: https
      - args:
        - --health-probe-bind-address=:8081
        - --metrics-bind-address=127.0.0.1:8080
        - --leader-elect
        command:
        - /manager
        env:
        - name: ACCOP_LOG_LEVEL
          value: "2"
        image: [your_registry_path]/acc-operator:[version x.y.z]
        imagePullPolicy: IfNotPresent
      imagePullSecrets: []
```

3. Astra Control Center 운영자를 설치합니다.

```
kubectl apply -f astra_control_center_operator_deploy.yaml
```

샘플 반응:

```
namespace/netapp-acc-operator created
customresourcedefinition.apiextensions.k8s.io/astracontrolcenters.astra.
netapp.io created
role.rbac.authorization.k8s.io/acc-operator-leader-election-role created
clusterrole.rbac.authorization.k8s.io/acc-operator-manager-role created
clusterrole.rbac.authorization.k8s.io/acc-operator-metrics-reader
created
clusterrole.rbac.authorization.k8s.io/acc-operator-proxy-role created
rolebinding.rbac.authorization.k8s.io/acc-operator-leader-election-
rolebinding created
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-manager-
rolebinding created
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-proxy-
rolebinding created
configmap/acc-operator-manager-config created
service/acc-operator-controller-manager-metrics-service created
deployment.apps/acc-operator-controller-manager created
```

4. Pod가 실행 중인지 확인합니다.

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

Astra Control Center를 구성합니다

1. Astra Control Center 사용자 정의 리소스(CR) 파일을 편집합니다 (`astra_control_center_min.yaml`) 계정, AutoSupport, 레지스트리 및 기타 필요한 구성을 만들려면:

> `astra_control_center_min.yaml` 기본 CR이며 대부분의 설치에 적합합니다. 모든 것을 숙지합니다 "CR 옵션 및 잠재적 가치" 고객의 환경에 맞게 Astra Control Center를 올바르게 구축할 수 있습니다. 사용자 환경에 추가 사용자 지정이 필요한 경우 를 사용할 수 있습니다 `astra_control_center.yaml` 대체 CR입니다.

```
vim astra_control_center_min.yaml
```

> 인증이 필요하지 않은 레지스트리를 사용하는 경우 을 삭제해야 합니다 `secret` 줄 내부 `imageRegistry` 그렇지 않으면 설치가 실패합니다.

a. 변경 `[your_registry_path]` 이전 단계에서 이미지를 푸시한 레지스트리 경로로 이동합니다.

b. 를 변경합니다 `accountName` 계정에 연결할 이름에 대한 문자열입니다.

c. 를 변경합니다 `astraAddress` 브라우저에서 Astra에 액세스하기 위해 사용할 FQDN에 대한 문자열입니다.

사용하지 마십시오 `http://` 또는 `https://` 를 입력합니다. 에서 사용하기 위해 이 FQDN을 복사합니다 나중에.

d. 를 변경합니다 `email` 문자열을 기본 초기 관리자 주소로 설정합니다. 에서 사용할 이 이메일 주소를 복사합니다 나중에.

e. 변경 `enrolled` 을 눌러 AutoSupport to로 이동합니다 `false` 인터넷 연결이 없거나 보관되지 않은 사이트의 경우 `true` 연결된 사이트의 경우.

f. 외부 인증서 관리자를 사용하는 경우 에 다음 행을 추가합니다 `spec`:

```
spec:
  crds:
    externalCertManager: true
```

g. (선택 사항) 이름을 추가합니다 `firstName` 성을 입력합니다 `lastName` 계정에 연결된 사용자의 입니다. UI 내에서 이 단계를 지금 또는 나중에 수행할 수 있습니다.

h. (선택 사항) 을 변경합니다 `storageClass` 설치에 필요한 경우 다른 Trident storageClass 리소스에 대한 값입니다.

i. (선택 사항) 설치 후 클러스터를 Astra Control Center에서 자동으로 관리하려는 경우 이 클러스터에 kubecon무화과 같은 암호를 만들었습니다, 라는 이 YAML 파일에 새 필드를 추가하여 비밀의 이름을 입력합니다 `astraKubeConfigSecret: "acc-kubeconfig-cred or custom secret name"`

j. 다음 단계 중 하나를 수행합니다.

- * 기타 수신 컨트롤러(ingressType: Generic) *: Astra Control Center의 기본 동작입니다. Astra Control Center를 배포한 후 URL을 사용하여 Astra Control Center를 노출하도록 수신 컨트롤러를 구성해야 합니다.

  기본 Astra Control Center 설치는 게이트웨이를 설정합니다 (`service/traefik`)를 입력합니다 `ClusterIP`. 이 기본 설치에서는 트래픽을 이 컨트롤러로 라우팅하기 위해 추가적으로 Kubernetes IngPressController/Ingress를 설정해야 합니다. 침투를 사용하려면 를 참조하십시오 "부하 분산을 위한 수신 설정".

- * 서비스 로드 밸런서(ingressType:AccTraefik) *: IngressController를 설치하거나 수신 리소스를 생성하지 않으려면 를 설정합니다 `ingressType` 를 선택합니다 `AccTraefik`.

  그러면 Astra Control Center가 구축됩니다 `traefik` Kubernetes 로드 밸런서 유형 서비스로서의 게이트웨이

  Astra Control Center는 "loadbalancer" 유형의 서비스를 사용합니다. (`svc/traefik` Astra Control Center 네임스페이스에서), 액세스 가능한 외부 IP 주소를 할당해야 합니다. 로드 밸런서가 사용자 환경에서 허용되고 아직 로드 밸런서가 구성되어 있지 않은 경우 MetalLB 또는 다른 외부 서비스 로드 밸런서를 사용하여 외부 IP 주소를 서비스에 할당할 수 있습니다. 내부 DNS 서버 구성에서 Astra Control Center에 대해 선택한 DNS 이름을 부하 분산 IP 주소로 지정해야 합니다.

> "로드 밸런서" 및 수신 서비스 유형에 대한 자세한 내용은 을 참조하십시오 "요구 사항".

```
apiVersion: astra.netapp.io/v1
kind: AstraControlCenter
metadata:
  name: astra
spec:
  accountName: "Example"
  astraVersion: "ASTRA_VERSION"
  astraAddress: "astra.example.com"
  astraKubeConfigSecret: "acc-kubeconfig-cred or custom secret name"
  ingressType: "Generic"
  autoSupport:
    enrolled: true
  email: "[admin@example.com]"
  firstName: "SRE"
  lastName: "Admin"
  imageRegistry:
    name: "[your_registry_path]"
    secret: "astra-registry-cred"
  storageClass: "ontap-gold"
```

Astra 제어 센터 및 운전자 설치를 완료합니다

1. 이전 단계에서 아직 작성하지 않은 경우 를 만듭니다 `netapp-acc` (또는 사용자 지정) 네임스페이스:

   ```
   kubectl create ns [netapp-acc or custom namespace]
   ```

   샘플 반응:

   ```
   namespace/netapp-acc created
   ```

2. 에 Astra Control Center를 설치합니다 `netapp-acc` (또는 사용자 지정) 네임스페이스:

   ```
   kubectl apply -f astra_control_center_min.yaml -n [netapp-acc or custom
   namespace]
   ```

   샘플 반응:

   ```
   astracontrolcenter.astra.netapp.io/astra created
   ```

시스템 상태를 확인합니다

OpenShift를 사용하려는 경우 검증 단계에 유사한 OC 명령을 사용할 수 있습니다.

1. 모든 시스템 구성 요소가 성공적으로 설치되었는지 확인합니다.

```
kubectl get pods -n [netapp-acc or custom namespace]
```

각 POD의 상태는 입니다 `Running`. 시스템 포드를 구축하는 데 몇 분 정도 걸릴 수 있습니다.

샘플 응답

```
NAME                                        READY   STATUS    RESTARTS
AGE
acc-helm-repo-6b44d68d94-d8m55              1/1     Running   0
13m
activity-78f99ddf8-hltct                    1/1     Running   0
10m
api-token-authentication-457nl              1/1     Running   0
9m28s
api-token-authentication-dgwsz              1/1     Running   0
9m28s
api-token-authentication-hmqqc              1/1     Running   0
9m28s
asup-75fd554dc6-m6qzh                       1/1     Running   0
9m38s
authentication-6779b4c85d-92gds             1/1     Running   0
8m11s
bucketservice-7cc767f8f8-lqwr8              1/1     Running   0
9m31s
certificates-549fd5d6cb-5kmd6               1/1     Running   0
9m56s
certificates-549fd5d6cb-bkjh9               1/1     Running   0
9m56s
cloud-extension-7bcb7948b-hn8h2             1/1     Running   0
10m
cloud-insights-service-56ccf86647-fgg69     1/1     Running   0
9m46s
composite-compute-677685b9bb-7vgsf          1/1     Running   0
10m
composite-volume-657d6c5585-dnq79           1/1     Running   0
9m49s
credentials-755fd867c8-vrlmt                1/1     Running   0
11m
entitlement-86495cdf5b-nwhh2                1/1     Running   2
10m
features-5684fb8b56-8d6s8                   1/1     Running   0
10m
fluent-bit-ds-rhx7v                         1/1     Running   0
7m48s
fluent-bit-ds-rjms4                         1/1     Running   0
7m48s
fluent-bit-ds-zf5ph                         1/1     Running   0
7m48s
graphql-server-66d895f544-w6hjd             1/1     Running   0
```

```
3m29s
identity-744df448d5-rlcmm                1/1     Running   0
10m
influxdb2-0                              1/1     Running   0
13m
keycloak-operator-75c965cc54-z7csw       1/1     Running   0
8m16s
krakend-798d6df96f-9z2sk                 1/1     Running   0
3m26s
license-5fb7d75765-f8mjg                 1/1     Running   0
9m50s
login-ui-7d5b7df85d-l2s7s                1/1     Running   0
3m20s
loki-0                                   1/1     Running   0
13m
metrics-facade-599b9d7fcc-gtmgl          1/1     Running   0
9m40s
monitoring-operator-67cc74f844-cdplp     2/2     Running   0
8m11s
nats-0                                   1/1     Running   0
13m
nats-1                                   1/1     Running   0
13m
nats-2                                   1/1     Running   0
12m
nautilus-769f5b74cd-k5jxm                1/1     Running   0
9m42s
nautilus-769f5b74cd-kd9gd                1/1     Running   0
8m59s
openapi-84f6ccd8ff-76kvp                 1/1     Running   0
9m34s
packages-6f59fc67dc-4g2f5                1/1     Running   0
9m52s
polaris-consul-consul-server-0           1/1     Running   0
13m
polaris-consul-consul-server-1           1/1     Running   0
13m
polaris-consul-consul-server-2           1/1     Running   0
13m
polaris-keycloak-0                       1/1     Running   0
8m7s
polaris-keycloak-1                       1/1     Running   0
5m49s
polaris-keycloak-2                       1/1     Running   0
5m15s
polaris-keycloak-db-0                    1/1     Running   0
```

```
8m6s
polaris-keycloak-db-1                     1/1     Running   0
5m49s
polaris-keycloak-db-2                     1/1     Running   0
4m57s
polaris-mongodb-0                         2/2     Running   0
13m
polaris-mongodb-1                         2/2     Running   0
12m
polaris-mongodb-2                         2/2     Running   0
12m
polaris-ui-565f56bf7b-zwr8b               1/1     Running   0
3m19s
polaris-vault-0                           1/1     Running   0
13m
polaris-vault-1                           1/1     Running   0
13m
polaris-vault-2                           1/1     Running   0
13m
public-metrics-6d86d66444-2wbzl           1/1     Running   0
9m30s
storage-backend-metrics-77c5d98dcd-dbhg5 1/1     Running   0
9m44s
storage-provider-78c885f57c-6zcv4         1/1     Running   0
9m36s
telegraf-ds-2l2m9                         1/1     Running   0
7m48s
telegraf-ds-qfzgh                         1/1     Running   0
7m48s
telegraf-ds-shrms                         1/1     Running   0
7m48s
telegraf-rs-bjpkt                         1/1     Running   0
7m48s
telemetry-service-6684696c64-qzfdf        1/1     Running   0
10m
tenancy-6596b6c54d-vmpsm                  1/1     Running   0
10m
traefik-7489dc59f9-6mnst                  1/1     Running   0
3m19s
traefik-7489dc59f9-xrkgg                  1/1     Running   0
3m4s
trident-svc-6c8dc458f5-jswcl              1/1     Running   0
10m
vault-controller-6b954f9b76-gz9nm         1/1     Running   0
11m
```

2. (선택 사항) 설치가 완료되었는지 확인하기 위해 을(를) 볼 수 있습니다 `acc-operator` 다음 명령을 사용하여 기록합니다.

```
kubectl logs deploy/acc-operator-controller-manager -n netapp-acc-
operator -c manager -f
```

> `accHost` 클러스터 등록은 마지막 작업 중 하나이며, 클러스터 등록에 실패하면 배포에 실패하지 않습니다. 로그에 클러스터 등록 실패가 표시되는 경우 클러스터 추가 워크플로우를 통해 등록을 다시 시도할 수 있습니다 "를 클릭합니다" API를 사용합니다.

3. 모든 Pod가 실행되면 설치가 성공적으로 완료되었는지 확인합니다 (`READY` 있습니다 `True`)를 입력하고 Astra Control Center에 로그인할 때 사용할 일회용 암호를 받습니다.

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

응답:

```
NAME    UUID                                        VERSION     ADDRESS
READY
astra   ACC-9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f  22.08.1-26
10.111.111.111  True
```

> UUID 값을 복사합니다. 암호는 입니다 `ACC-` UUID 값 뒤에 옵니다 (`ACC-[UUID]` 또는, 이 예에서는 `ACC-9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f`)를 클릭합니다.

부하 분산을 위한 수신 설정

클러스터의 로드 밸런싱과 같은 서비스에 대한 외부 액세스를 관리하는 Kubernetes 수신 컨트롤러를 설정할 수 있습니다.

이 절차에서는 수신 컨트롤러를 설정하는 방법에 대해 설명합니다 (`ingressType:Generic`)를 클릭합니다. 이것은 Astra Control Center의 기본 동작입니다. Astra Control Center를 배포한 후 URL을 사용하여 Astra Control Center를 노출하도록 수신 컨트롤러를 구성해야 합니다.

> 수신 컨트롤러를 설정하지 않으려면 을 설정할 수 있습니다 `ingressType:AccTraefik)`. Astra Control Center는 "loadbalancer" 유형의 서비스를 사용합니다. (`svc/traefik` Astra Control Center 네임스페이스에서), 액세스 가능한 외부 IP 주소를 할당해야 합니다. 로드 밸런서가 사용자 환경에서 허용되고 아직 로드 밸런서가 구성되어 있지 않은 경우 MetalLB 또는 다른 외부 서비스 로드 밸런서를 사용하여 외부 IP 주소를 서비스에 할당할 수 있습니다. 내부 DNS 서버 구성에서 Astra Control Center에 대해 선택한 DNS 이름을 부하 분산 IP 주소로 지정해야 합니다. "로드 밸런서" 및 수신 서비스 유형에 대한 자세한 내용은 을 참조하십시오 "요구 사항".

단계는 사용하는 수신 컨트롤러의 유형에 따라 다릅니다.

- 이스티오 침투

- Nginx 수신 컨트롤러
- OpenShift 수신 컨트롤러

필요한 것

- 필수 요소입니다 "수신 컨트롤러" 이미 배포되어 있어야 합니다.
- 를 클릭합니다 "수신 클래스" 수신 컨트롤러에 해당하는 컨트롤러가 이미 생성되어야 합니다.
- V1.19 및 v1.22 등의 Kubernetes 버전을 사용하고 있습니다.

Istio 침투에 대한 단계

1. Istio Ingress를 구성합니다.

   이 절차에서는 "기본" 구성 프로파일을 사용하여 Istio를 구축한다고 가정합니다.

2. 수신 게이트웨이에 대해 원하는 인증서 및 개인 키 파일을 수집하거나 생성합니다.

   CA 서명 또는 자체 서명 인증서를 사용할 수 있습니다. 공통 이름은 Astra 주소(FQDN)여야 합니다.

   명령 예:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048
-keyout tls.key -out tls.crt
```

3. 암호를 만듭니다 `tls secret name` 유형 `kubernetes.io/tls` 에서 TLS 개인 키 및 인증서의 경우 `istio-system namespace` TLS 비밀에 설명되어 있습니다.

   명령 예:

```
kubectl create secret tls [tls secret name]
--key="tls.key"
--cert="tls.crt" -n istio-system
```

   비밀의 이름은 과 일치해야 합니다 `spec.tls.secretName` 에 제공됩니다 `istio-ingress.yaml` 파일.

4. 수신 리소스를 에 배포합니다 `netapp-acc` v1beta1(또는 1.22 미만의 Kubernetes 버전에서 사용되지 않음) 또는 v1 리소스 유형을 사용하는(또는 사용자 지정 이름) 네임스페이스입니다.

   출력:

```yaml
apiVersion: networking.k8s.io/v1beta1
kind: IngressClass
metadata:
  name: istio
spec:
  controller: istio.io/ingress-controller
---
apiVersion: networking.k8s.io/v1beta1
kind: Ingress
metadata:
  name: ingress
  namespace: istio-system
spec:
  ingressClassName: istio
  tls:
  - hosts:
    - <ACC addess>
    secretName: [tls secret name]
  rules:
  - host: [ACC addess]
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          serviceName: traefik
          servicePort: 80
```

v1 새 스키마의 경우 다음 샘플을 따르십시오.

```
kubectl apply -f istio-Ingress.yaml
```

출력:

```
apiVersion: networking.k8s.io/v1
kind: IngressClass
metadata:
  name: istio
spec:
  controller: istio.io/ingress-controller
---
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: ingress
  namespace: istio-system
spec:
  ingressClassName: istio
  tls:
  - hosts:
    - <ACC addess>
    secretName: [tls secret name]
  rules:
  - host: [ACC addess]
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          service:
            name: traefik
            port:
              number: 80
```

5. Astra Control Center를 평소처럼 배포합니다.
6. 수신 상태를 점검하십시오.

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

응답:

```
NAME    CLASS HOSTS              ADDRESS         PORTS   AGE
ingress istio astra.example.com 172.16.103.248  80, 443 1h
```

Nginx 수신 컨트롤러 단계

1. 형식의 암호를 만듭니다[`kubernetes.io/tls`] 에서 TLS 개인 키 및 인증서의 경우 `netapp-acc` 에 설명된

대로 (또는 사용자 지정 이름) 네임스페이스를 사용합니다 "TLS 비밀".

2. 수신 리소스를 에 배포합니다 `netapp-acc` 또는 사용자 지정 이름 네임스페이스 중 하나를 사용합니다 `v1beta1` (Kubernetes 버전 1.22 이하) 또는 에서는 사용되지 않습니다 `v1` 사용되지 않는 스키마나 새 스키마의 리소스 유형:

   a. 을(를) 위한 `v1beta1` 더 이상 사용되지 않는 스키마는 다음 샘플을 따르십시오.

```
apiVersion: extensions/v1beta1
Kind: IngressClass
metadata:
  name: ingress-acc
  namespace: [netapp-acc or custom namespace]
  annotations:
    kubernetes.io/ingress.class: [class name for nginx controller]
spec:
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: [ACC address]
    http:
      paths:
      - backend:
        serviceName: traefik
        servicePort: 80
        pathType: ImplementationSpecific
```

   b. 의 경우 `v1` 새 스키마에 따라 다음 샘플을 수행합니다.

```yaml
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: netapp-acc-ingress
  namespace: [netapp-acc or custom namespace]
spec:
  ingressClassName: [class name for nginx controller]
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: <ACC addess>
    http:
      paths:
        - path:
          backend:
            service:
              name: traefik
              port:
                number: 80
          pathType: ImplementationSpecific
```

OpenShift Ingress 컨트롤러를 위한 단계

1. 인증서를 구입하고 OpenShift 라우트에서 사용할 수 있도록 준비된 키, 인증서 및 CA 파일을 가져옵니다.
2. OpenShift 경로를 생성합니다.

```
oc create route edge --service=traefik
--port=web -n [netapp-acc or custom namespace]
--insecure-policy=Redirect --hostname=<ACC address>
--cert=cert.pem --key=key.pem
```

Astra Control Center UI에 로그인합니다

Astra Control Center를 설치한 후 기본 관리자의 암호를 변경하고 Astra Control Center UI 대시보드에 로그인합니다.

단계

1. 브라우저에서 에 사용한 FQDN을 입력합니다 `astraAddress` 에 있습니다 `astra_control_center_min.yaml` CR Astra Control Center를 설치했습니다.
2. 메시지가 표시되면 자체 서명된 인증서를 수락합니다.

> 로그인 후 사용자 지정 인증서를 만들 수 있습니다.

3. Astra Control Center 로그인 페이지에서 에 사용한 값을 입력합니다 `email` 인치 `astra_control_center_min.yaml` CR Astra Control Center를 설치했습니다1회 암호 뒤에 옵니다 (`ACC-[UUID]`)를 클릭합니다.

> 잘못된 암호를 세 번 입력하면 15분 동안 관리자 계정이 잠깁니다.

4. Login * 을 선택합니다.
5. 메시지가 나타나면 암호를 변경합니다.

> 처음 로그인하는 데 암호를 잊은 경우 다른 관리 사용자 계정이 아직 생성되지 않은 경우 NetApp 지원에 암호 복구 지원을 문의하십시오.

6. (선택 사항) 기존의 자체 서명된 TLS 인증서를 제거하고 로 바꿉니다 "인증 기관(CA)에서 서명한 사용자 지정 TLS 인증서".

설치 문제를 해결합니다

에 서비스가 있는 경우 `Error` 상태, 로그를 검사할 수 있습니다. 400 ~ 500 범위의 API 응답 코드를 찾습니다. 이는 고장이 발생한 장소를 나타냅니다.

단계

1. Astra Control Center 운영자 로그를 검사하려면 다음을 입력하십시오.

```
kubectl logs --follow -n netapp-acc-operator $(kubectl get pods -n
netapp-acc-operator -o name) -c manager
```

다음 단계

를 수행하여 배포를 완료합니다 "설정 작업".

=
:allow-uri-read:

POD 보안 정책 제한 사항 이해

Astra Control Center는 POD 보안 정책(PSP)을 통해 권한 제한을 지원합니다. POD 보안 정책을 사용하면 컨테이너를 실행할 수 있는 사용자 또는 그룹과 해당 컨테이너에 사용할 수 있는 권한을 제한할 수 있습니다.

RKE2와 같은 일부 Kubernetes 배포에는 기본 POD 보안 정책이 너무 제한적이며 Astra Control Center 설치 시 문제가 발생합니다.

여기에 포함된 정보와 예제를 사용하여 Astra Control Center가 생성하는 POD 보안 정책을 이해하고, Astra Control Center 기능을 방해하지 않으면서 필요한 보호 기능을 제공하는 POD 보안 정책을 구성할 수 있습니다.

Astra Control Center에서 설치한 **PSP**

Astra Control Center는 설치 중에 몇 가지 POD 보안 정책을 생성합니다. 이 중 일부는 영구적이며 일부 작업은 특정 작업 중에 생성되며 작업이 완료되면 제거됩니다.

설치 중에 **PSP**가 생성되었습니다

Astra Control Center를 설치하는 동안 Astra Control Center 운영자는 사용자 지정 POD 보안 정책, 역할 개체 및 RoleBinding 개체를 설치하여 Astra Control Center 네임스페이스에 Astra Control Center 서비스를 배포할 수 있도록 합니다.

새 정책 및 객체에는 다음과 같은 특성이 있습니다.

```
kubectl get psp

NAME                            PRIV    CAPS          SELINUX    RUNASUSER
FSGROUP     SUPGROUP    READONLYROOTFS   VOLUMES
avp-psp                         false                 RunAsAny   RunAsAny
RunAsAny    RunAsAny    false            *
netapp-astra-deployment-psp     false                 RunAsAny   RunAsAny
RunAsAny    RunAsAny    false            *

kubectl get role

NAME                                     CREATED AT
netapp-astra-deployment-role             2022-06-27T19:34:58Z

kubectl get rolebinding

NAME                                     ROLE
AGE
netapp-astra-deployment-rb               Role/netapp-astra-deployment-role
32m
```

백업 작업 중에 **PSP**가 생성되었습니다

백업 작업 중에 Astra Control Center는 동적 POD 보안 정책, ClusterRole 개체 및 RoleBinding 개체를 만듭니다. 이러한 백업 프로세스는 별도의 네임스페이스에서 수행됩니다.

새 정책 및 객체에는 다음과 같은 특성이 있습니다.

```
kubectl get psp

NAME                            PRIV    CAPS
SELINUX    RUNASUSER          FSGROUP     SUPGROUP    READONLYROOTFS
VOLUMES
netapp-astra-backup             false   DAC_READ_SEARCH
RunAsAny   RunAsAny           RunAsAny    RunAsAny    false            *

kubectl get role

NAME                  CREATED AT
netapp-astra-backup   2022-07-21T00:00:00Z

kubectl get rolebinding

NAME                  ROLE                        AGE
netapp-astra-backup   Role/netapp-astra-backup   62s
```

클러스터 관리 중에 생성된 **PSP**입니다

클러스터를 관리할 때 Astra Control Center는 NetApp 모니터링 연산자를 관리형 클러스터에 설치합니다. 이 연산자는 POD 보안 정책, ClusterRole 개체 및 RoleBinding 개체를 만들어 Astra Control Center 네임스페이스에 원격 측정 서비스를 배포합니다.

새 정책 및 객체에는 다음과 같은 특성이 있습니다.

```
kubectl get psp

NAME                            PRIV    CAPS
SELINUX    RUNASUSER          FSGROUP     SUPGROUP    READONLYROOTFS
VOLUMES
netapp-monitoring-psp-nkmo      true    AUDIT_WRITE,NET_ADMIN,NET_RAW
RunAsAny   RunAsAny           RunAsAny    RunAsAny    false            *

kubectl get role

NAME                                          CREATED AT
netapp-monitoring-role-privileged             2022-07-21T00:00:00Z

kubectl get rolebinding

NAME                                                    ROLE
AGE
netapp-monitoring-role-binding-privileged               Role/netapp-
monitoring-role-privileged              2m5s
```

일부 환경에서는 NetworkPolicy 구문을 사용하여 네임스페이스 간 트래픽을 제한합니다. Astra Control Center 운영자, Astra Control Center 및 VMware vSphere용 Astra Plugin은 모두 서로 다른 네임스페이스에 있습니다. 서로 다른 네임스페이스에 있는 서비스는 서로 통신할 수 있어야 합니다. 이 통신을 활성화하려면 다음 단계를 수행하십시오.

단계

1. Astra Control Center 네임스페이스에 있는 NetworkPolicy 리소스를 삭제합니다.

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

2. 앞의 명령으로 반환된 각 NetworkPolicy 개체에 대해 다음 명령을 사용하여 개체를 삭제합니다. object_name>을(를) 반환된 개체의 이름으로 바꿉니다.

```
kubectl delete networkpolicy <OBJECT_NAME> -n netapp-acc
```

3. Astra Plugin for VMware vSphere 서비스가 Astra Control Center 서비스에 요청을 할 수 있도록 acc-AVP-network-policy 객체를 구성하려면 다음 리소스 파일을 적용하십시오. 괄호 <>의 정보를 사용자 환경의 정보로 바꿉니다.

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: acc-avp-network-policy
  namespace: <ACC_NAMESPACE_NAME> # REPLACE THIS WITH THE ASTRA CONTROL
CENTER NAMESPACE NAME
spec:
  podSelector: {}
  policyTypes:
    - Ingress
  ingress:
    - from:
        - namespaceSelector:
            matchLabels:
              kubernetes.io/metadata.name: <PLUGIN_NAMESPACE_NAME> #
REPLACE THIS WITH THE ASTRA PLUGIN FOR VMWARE VSPHERE NAMESPACE NAME
```

4. 다음 리소스 파일을 적용하여 Astra Control Center 운영자가 Astra Control Center 서비스와 통신할 수 있도록 acc-operator-network-policy 객체를 구성합니다. 괄호 <>의 정보를 사용자 환경의 정보로 바꿉니다.

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: acc-operator-network-policy
  namespace: <ACC_NAMESPACE_NAME> # REPLACE THIS WITH THE ASTRA CONTROL
CENTER NAMESPACE NAME
spec:
  podSelector: {}
  policyTypes:
    - Ingress
  ingress:
    - from:
        - namespaceSelector:
            matchLabels:
              kubernetes.io/metadata.name: <NETAPP-ACC-OPERATOR> #
REPLACE THIS WITH THE OPERATOR NAMESPACE NAME
```

리소스 제한을 제거합니다

일부 환경에서는 ResourceQuotas 및 LimitRanges 개체를 사용하여 네임스페이스의 리소스가 클러스터에서 사용 가능한 모든 CPU 및 메모리를 사용하지 못하도록 합니다. Astra Control Center는 최대 제한을 설정하지 않으므로 해당 리소스를 준수하지 않습니다. Astra Control Center를 설치할 네임스페이스에서 제거해야 합니다.

다음 단계를 사용하여 할당량 및 제한을 검색하고 제거할 수 있습니다. 이 예제에서 명령 출력은 명령 직후에 표시됩니다.

단계

1. NetApp-acc 네임스페이스에서 리소스 할당량 확인:

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

응답:

```
NAME          AGE   REQUEST                                          LIMIT
pods-high     16s   requests.cpu: 0/20, requests.memory: 0/100Gi
limits.cpu: 0/200, limits.memory: 0/1000Gi
pods-low      15s   requests.cpu: 0/1, requests.memory: 0/1Gi
limits.cpu: 0/2, limits.memory: 0/2Gi
pods-medium   16s   requests.cpu: 0/10, requests.memory: 0/20Gi
limits.cpu: 0/20, limits.memory: 0/200Gi
```

2. 이름으로 모든 리소스 할당량 삭제:

```
kubectl delete resourcequota  pods-high -n netapp-acc
```

```
kubectl delete resourcequota  pods-low -n netapp-acc
```

```
kubectl delete resourcequota  pods-medium -n netapp-acc
```

3. NetApp-acc 네임스페이스의 제한 범위를 가져옵니다.

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

응답:

```
NAME               CREATED AT
cpu-limit-range    2022-06-27T19:01:23Z
```

4. 이름별로 제한 범위를 삭제합니다.

```
kubectl delete limitrange cpu-limit-range -n netapp-acc
```

=
:allow-uri-read:

OpenShift OperatorHub를 사용하여 Astra Control Center를 설치합니다

Red Hat OpenShift를 사용하는 경우 Red Hat 공인 운영자를 사용하여 Astra Control Center를 설치할 수 있습니다. 이 절차를 사용하여 에서 Astra Control Center를 설치합니다 "Red Hat 에코시스템 카탈로그" 또는 Red Hat OpenShift Container Platform 사용.

이 절차를 완료한 후에는 설치 절차로 돌아가 를 완료해야 합니다 "나머지 단계" 설치 성공 여부를 확인하고 로그온합니다.

필요한 것

- "설치를 시작하기 전에 Astra Control Center 구축을 위한 환경을 준비합니다".
- OpenShift 클러스터에서 모든 클러스터 운영자가 양호한 상태인지 확인합니다 (`available` 있습니다 `true`):

```
oc get clusteroperators
```

- OpenShift 클러스터에서 모든 API 서비스가 정상 상태인지 확인합니다 (`available` 있습니다 `true`):

```
oc get apiservices
```

- 데이터 센터에서 Astra Control Center에 대한 FQDN 주소를 생성합니다.
- 필요한 사용 권한을 얻고 Red Hat OpenShift Container Platform에 액세스하여 설명된 설치 단계를 수행합니다.
- 클러스터에 인증서 관리자가 이미 있는 경우 일부를 수행해야 합니다 "필수 단계" 따라서 Astra Control Center는 자체 인증 관리자를 설치하지 않습니다.

단계

- Astra Control Center 번들을 다운로드하고 포장을 풉니다
- NetApp Astra kubtl 플러그인을 설치합니다
- 이미지를 로컬 레지스트리에 추가합니다
- 운영자 설치 페이지를 찾으십시오
- 운전자를 설치합니다
- Astra Control Center를 설치합니다

Astra Control Center 번들을 다운로드하고 포장을 풉니다

1. Astra Control Center 번들을 다운로드합니다 (`astra-control-center-[version].tar.gz`)를 선택합니다 "NetApp Support 사이트".
2. 에서 Astra Control Center 인증서 및 키의 지퍼를 다운로드합니다 "NetApp Support 사이트".
3. (선택 사항) 다음 명령을 사용하여 번들의 서명을 확인합니다.

```
openssl dgst -sha256 -verify AstraControlCenter-public.pub -signature
astra-control-center-[version].tar.gz.sig astra-control-center-
[version].tar.gz
```

4. 이미지 추출:

```
tar -vxzf astra-control-center-[version].tar.gz
```

NetApp Astra kubtl 플러그인을 설치합니다

NetApp 아스트라 `kubectl` 명령줄 플러그인을 사용하면 Astra Control Center 배포 및 업그레이드와 관련된 일반적인 작업을 수행할 때 시간을 절약할 수 있습니다.

필요한 것

NetApp은 다양한 CPU 아키텍처 및 운영 체제용 플러그인의 바이너리를 제공합니다. 이 작업을 수행하기 전에 사용 중인 CPU 및 운영 체제를 알아야 합니다. Linux 및 Mac 운영 체제에서는 를 사용할 수 있습니다 `uname -a` 명령을 사용하여 이 정보를 수집합니다.

단계

1. 사용 가능한 NetApp Astra를 나열하십시오 `kubectl` 플러그인 바이너리를 만들고 운영 체제 및 CPU 아키텍처에 필요한 파일 이름을 적어 둡니다.

```
ls kubectl-astra/
```

2. 파일을 규격과 같은 위치에 복사합니다 `kubectl` 유틸리티. 이 예에서 는 입니다 `kubectl` 유틸리티는 에 있습니다 `/usr/local/bin` 디렉토리. 대치 `<binary-name>` 필요한 파일 이름:

```
cp kubectl-astra/<binary-name> /usr/local/bin/kubectl-astra
```

이미지를 로컬 레지스트리에 추가합니다

1. 용기 엔진에 적합한 단계 시퀀스를 완료합니다.

Docker 를 참조하십시오

1. Astra 디렉토리로 이동합니다.

```
cd acc
```

2. Astra Control Center 이미지 디렉토리에 있는 패키지 이미지를 로컬 레지스트리로 푸시합니다. 명령을 실행하기 전에 다음 대체 작업을 수행합니다.
   - Bundle_file을 Astra Control 번들 파일 이름으로 바꿉니다(예: `acc.manifest.yaml`)를 클릭합니다.
   - my_registry를 Docker 리포지토리의 URL로 바꿉니다.
   - my_registry_user를 사용자 이름으로 바꿉니다.
   - my_registry_token을 레지스트리에 대한 인증된 토큰으로 바꿉니다.

```
kubectl astra packages push-images -m BUNDLE_FILE -r MY_REGISTRY
-u MY_REGISTRY_USER -p MY_REGISTRY_TOKEN
```

팟맨

1. 레지스트리에 로그인합니다.

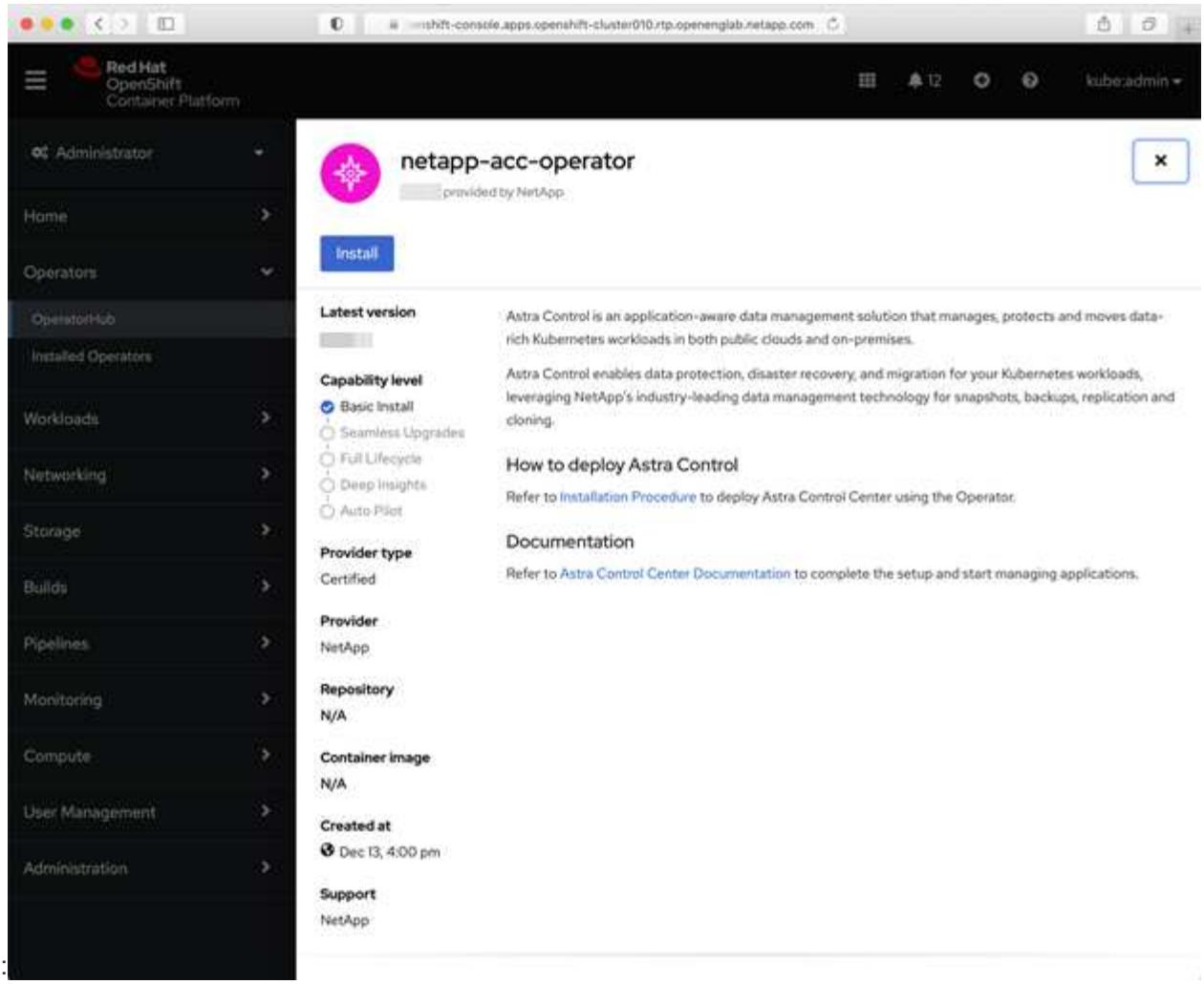
```
podman login [your_registry_path]
```

2. 설명에 명시된 대로 <your_registry> 대체를 만들어 다음 스크립트를 실행합니다.

```
# You need to be at the root of the tarball.
# You should see these files to confirm correct location:
#   acc.manifest.yaml
#   acc/

# Replace <YOUR_REGISTRY> with your own registry (e.g
registry.customer.com or registry.customer.com/testing, etc..)
export REGISTRY=<YOUR_REGISTRY>
export PACKAGENAME=acc
export PACKAGEVERSION=22.08.1-26
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
  # Load to local cache
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')

  # Remove path and keep imageName.
  astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')

  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/netapp/astra/${PACKAGENAME}
/${PACKAGEVERSION}/${astraImageNoPath}

  # Push to the local repo.
  podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done
```

운영자 설치 페이지를 찾으십시오

1. 운영자 설치 페이지에 액세스하려면 다음 절차 중 하나를 완료하십시오.
   - Red Hat OpenShift 웹 콘솔



:

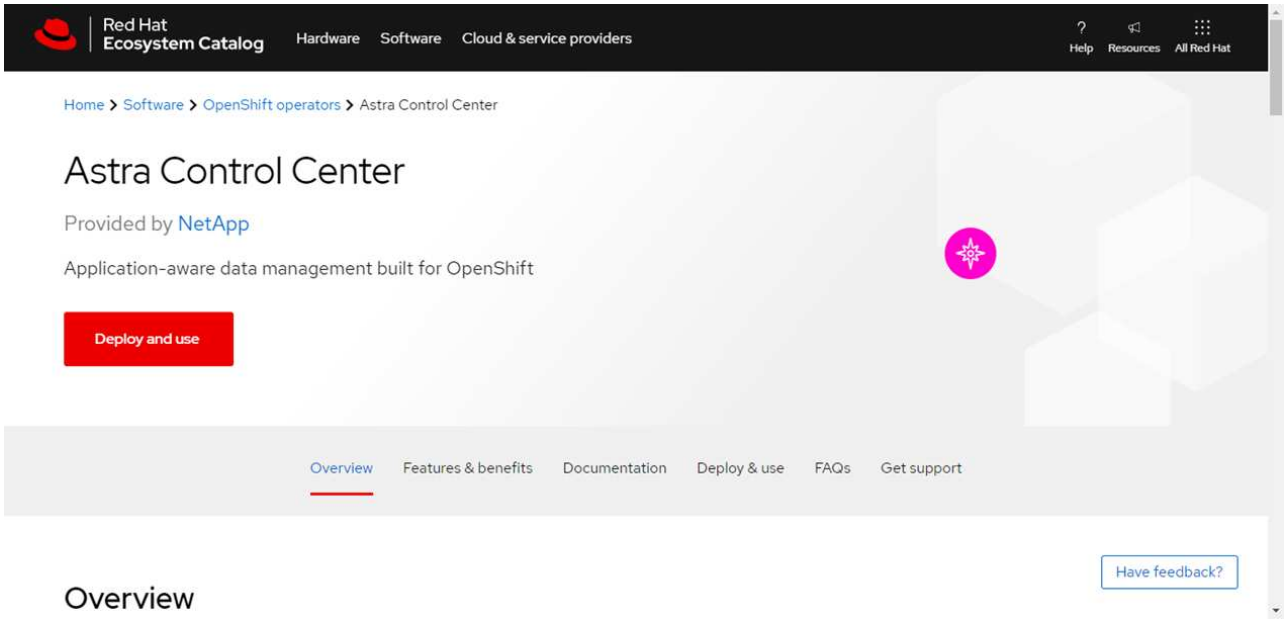
i. OpenShift Container Platform UI에 로그인합니다.

ii. 측면 메뉴에서 * Operators > OperatorHub * 를 선택합니다.

iii. NetApp Astra Control Center 운영자를 선택합니다.

iv. 설치 * 를 선택합니다.

- Red Hat 에코시스템 카탈로그
  :



i. NetApp Astra Control Center를 선택합니다 "운영자".

ii. 배포 및 사용 * 을 선택합니다.

운전자를 설치합니다

1. Install Operator * 페이지를 완료하고 운영자를 설치합니다.

> 운영자는 모든 클러스터 네임스페이스에서 사용할 수 있습니다.

a. 연산자 네임스페이스 또는 를 선택합니다 `netapp-acc-operator` 네임스페이스는 운영자 설치의 일부로 자동으로 생성됩니다.

b. 수동 또는 자동 승인 전략을 선택합니다.

> 수동 승인이 권장됩니다. 클러스터당 하나의 운영자 인스턴스만 실행 중이어야 합니다.

c. 설치 * 를 선택합니다.

> 수동 승인 전략을 선택한 경우 이 운영자에 대한 수동 설치 계획을 승인하라는 메시지가 표시됩니다.

2. 콘솔에서 OperatorHub 메뉴로 이동하여 운영자가 성공적으로 설치되었는지 확인합니다.

Astra Control Center를 설치합니다

1. Astra Control Center 운용자의 세부 정보 보기 내 콘솔에서 를 선택합니다 `Create instance` 제공된 API 섹션에서

2. 를 완료합니다 `Create AstraControlCenter` 양식 필드:

a. Astra Control Center 이름을 유지하거나 조정합니다.

b. (선택 사항) 자동 지원을 활성화 또는 비활성화합니다. 자동 지원 기능을 유지하는 것이 좋습니다.

c. Astra Control Center 주소를 입력합니다. 들어가지마 `http://` 또는 `https://` 를 입력합니다.

d. Astra Control Center 버전을 입력합니다(예: 21.12.60).

e. 계정 이름, 이메일 주소 및 관리자 성을 입력합니다.

f. 기본 볼륨 재확보 정책을 유지합니다.

g. 이미지 레지스트리 * 에서 로컬 컨테이너 이미지 레지스트리 경로를 입력합니다. 들어가지마 `http://` 또는 `https://` 를 입력합니다.

h. 인증이 필요한 레지스트리를 사용하는 경우 암호를 입력합니다.

i. 관리자의 이름을 입력합니다.

j. 리소스 확장을 구성합니다.

k. 기본 스토리지 클래스를 유지합니다.

l. CRD 처리 기본 설정을 정의합니다.

3. 를 선택합니다 `Create`.

다음 단계

Astra Control Center가 성공적으로 설치되었는지 확인하고 를 완료합니다 "나머지 단계" 를 눌러 로그인합니다. 또한 를 수행하여 배포를 완료합니다 "설정 작업".

Cloud Volumes ONTAP 스토리지 백엔드를 사용하여 Astra Control Center를 설치합니다

Astra Control Center를 사용하면 자체 관리되는 Kubernetes 클러스터 및 Cloud Volumes ONTAP 인스턴스가 있는 하이브리드 클라우드 환경에서 앱을 관리할 수 있습니다. 온프레미스 Kubernetes 클러스터 또는 클라우드 환경의 자가 관리 Kubernetes 클러스터 중 하나에 Astra Control Center를 구축할 수 있습니다.

이러한 구축 중 하나를 통해 Cloud Volumes ONTAP를 스토리지 백엔드로 사용하여 애플리케이션 데이터 관리 작업을 수행할 수 있습니다. S3 버킷을 백업 타겟으로 구성할 수도 있습니다.

AWS(Amazon Web Services), GCP(Google Cloud Platform) 및 Microsoft Azure에 Cloud Volumes ONTAP 스토리지 백엔드를 사용하여 Astra Control Center를 설치하려면 클라우드 환경에 따라 다음 단계를 수행하십시오.

- Amazon Web Services에 Astra Control Center를 구축합니다
- Google Cloud Platform에 Astra Control Center를 구축합니다
- Microsoft Azure에 Astra Control Center를 구축합니다

OCP(OpenShift Container Platform)와 같이 자체 관리되는 Kubernetes 클러스터를 사용하여 배포판에서 앱을 관리할 수 있습니다. 자가 관리 OCP 클러스터만 Astra Control Center 구축을 위해 검증되었습니다.

Amazon Web Services에 Astra Control Center를 구축합니다

AWS(Amazon Web Services) 퍼블릭 클라우드에서 호스팅되는 자가 관리형 Kubernetes 클러스터에 Astra Control Center를 구축할 수 있습니다.

AWS에 필요한 것

AWS에 Astra Control Center를 구축하기 전에 다음 항목이 필요합니다.

- Astra Control Center 라이센스. 을 참조하십시오 "Astra Control Center 라이센스 요구 사항".

- "Astra Control Center 요구 사항을 충족합니다".
- NetApp Cloud Central 계정
- OCP를 사용하는 경우 Red Hat OpenShift Container Platform(OCP) 권한(네임스페이스 수준에서 POD 생성)
- 버킷 및 커넥터를 생성할 수 있는 권한이 있는 AWS 자격 증명, 액세스 ID 및 비밀 키
- AWS 계정 ECR(Elastic Container Registry) 액세스 및 로그인
- Astra Control UI에 액세스하려면 AWS 호스팅 영역 및 Route 53 항목이 필요합니다

AWS의 운영 환경 요구사항

Astra Control Center에는 AWS를 위한 다음과 같은 운영 환경이 필요합니다.

- Red Hat OpenShift Container Platform 4.8

> Astra Control Center를 호스팅하기 위해 선택한 운영 환경이 환경 공식 문서에 설명된 기본 리소스 요구 사항을 충족하는지 확인합니다.

Astra Control Center에는 환경의 리소스 요구 사항 외에 다음과 같은 리소스가 필요합니다.

구성 요소	요구 사항
백엔드 **NetApp Cloud Volumes ONTAP** 스토리지 용량입니다	최소 300GB가 사용 가능합니다
작업자 노드**(AWS EC2** 요구사항**)**	총 3개 이상의 작업자 노드, vCPU 코어 4개, 12GB RAM
로드 밸런서	수신 트래픽을 운영 환경 클러스터의 서비스로 전송할 수 있도록 서비스 유형 "로드 밸런서"를 사용할 수 있습니다
FQDN	Astra Control Center의 FQDN을 부하 분산 IP 주소로 가리키는 방법
Astra Trident(NetApp Cloud Manager에서 **Kubernetes** 클러스터 검색의 일부로 설치됨**)**	Astra Trident 21.04 이상 설치 및 구성, NetApp ONTAP 버전 9.5 이상 버전을 스토리지 백엔드로 사용합니다
이미지 레지스트리	Astra Control Center 빌드 이미지를 푸시할 수 있는 AWS Elastic Container Registry와 같은 기존 개인 레지스트리가 있어야 합니다. 이미지를 업로드할 이미지 레지스트리의 URL을 제공해야 합니다. Astra Control Center에서 호스팅되는 클러스터와 관리 클러스터는 Resetic 기반 이미지를 사용하여 앱을 백업 및 복원할 수 있도록 동일한 이미지 레지스트리에 액세스할 수 있어야 합니다.

구성 요소	요구 사항
Astra Trident/ONTAP 구성	Astra Control Center에서는 스토리지 클래스를 생성하고 기본 스토리지 클래스로 설정해야 합니다. Astra Control Center는 Kubernetes 클러스터를 NetApp Cloud Manager로 가져올 때 생성되는 다음과 같은 ONTAP Kubernetes 스토리지 클래스를 지원합니다. Astra Trident에서 제공합니다. • `vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-ha-san csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-san csi.trident.netapp.io`

이러한 요구 사항에서는 Astra Control Center가 운영 환경에서 실행되는 유일한 애플리케이션이라고 가정합니다. 환경에서 추가 애플리케이션이 실행 중인 경우 이러한 최소 요구 사항을 적절히 조정합니다.

AWS 레지스트리 토큰은 12시간 후에 만료되며, 그 후에는 Docker 이미지 레지스트리 암호를 갱신해야 합니다.

AWS 구축 개요

Cloud Volumes ONTAP를 스토리지 백엔드로 사용하여 Astra Control Center for AWS를 설치하는 프로세스를 간략하게 소개합니다.

이러한 각 단계는 아래에 자세히 설명되어 있습니다.

1. IAM 권한이 충분한지 확인하십시오.
2. AWS에 RedHat OpenShift 클러스터를 설치합니다.
3. AWS 구성.
4. NetApp Cloud Manager 구성.
5. Astra Control Center를 설치합니다.

IAM 권한이 충분한지 확인하십시오

RedHat OpenShift 클러스터와 NetApp Cloud Manager Connector를 설치할 수 있도록 충분한 IAM 역할 및 권한이 있는지 확인합니다.

을 참조하십시오 "초기 AWS 자격 증명".

AWS에 RedHat OpenShift 클러스터를 설치합니다

AWS에 RedHat OpenShift Container Platform 클러스터를 설치합니다.

설치 지침은 를 참조하십시오 "OpenShift Container Platform에서 AWS에 클러스터 설치".

AWS 구성

그런 다음 AWS를 구성하여 가상 네트워크를 생성하고, EC2 컴퓨팅 인스턴스를 설정하고, AWS S3 버킷을 생성하고, ECR(Elastic Container Register)을 생성하여 Astra Control Center 이미지를 호스팅하고, 이 레지스트리로 이미지를 푸시합니다.

AWS 설명서에 따라 다음 단계를 완료하십시오. 을 참조하십시오 "AWS 설치 설명서".

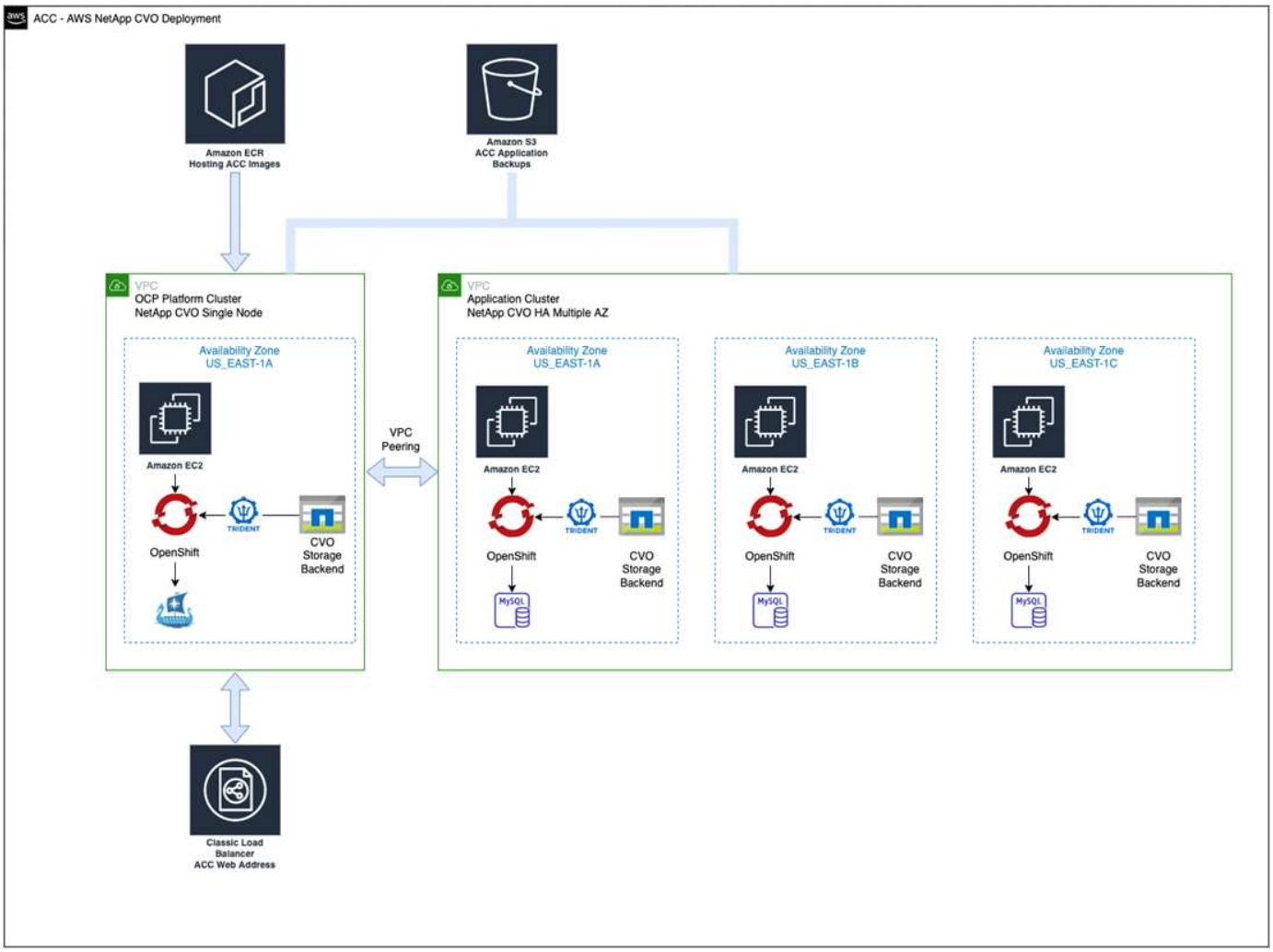
1. AWS 가상 네트워크를 생성합니다.
2. EC2 컴퓨팅 인스턴스를 검토합니다. 이는 AWS의 베어 메탈 서버 또는 VM이 될 수 있습니다.
3. 인스턴스 유형이 마스터 및 작업자 노드에 대한 Astra 최소 리소스 요구 사항과 일치하지 않으면 AWS의 인스턴스 유형을 Astra 요구 사항에 맞게 변경합니다. 을 참조하십시오 "Astra Control Center 요구 사항".
4. 백업을 저장할 AWS S3 버킷을 하나 이상 생성합니다.
5. AWS ECR(Elastic Container Registry)을 생성하여 모든 ACC 이미지를 호스팅합니다.

> ECR을 생성하지 않으면 Astra Control Center는 AWS 백엔드가 있는 Cloud Volumes ONTAP가 포함된 클러스터에서 모니터링 데이터에 액세스할 수 없습니다. 이 문제는 Astra Control Center를 사용하여 검색 및 관리하려는 클러스터에 AWS ECR 액세스 권한이 없을 때 발생합니다.

6. ACC 이미지를 정의된 레지스트리로 푸시합니다.

> AWS ECR(Elastic Container Registry) 토큰이 12시간 후에 만료되어 클러스터 간 클론 작업이 실패합니다. 이 문제는 AWS용으로 구성된 Cloud Volumes ONTAP에서 스토리지 백엔드를 관리할 때 발생합니다. 이 문제를 해결하려면 ECR을 다시 인증하고 클론 작업이 성공적으로 재개되도록 새로운 암호를 생성하십시오.

다음은 AWS 구축의 예입니다.



NetApp Cloud Manager 구성

Cloud Manager를 사용하여 작업 공간을 생성하고, AWS에 커넥터를 추가하고, 작업 환경을 생성하고, 클러스터를 가져옵니다.

Cloud Manager 설명서에 따라 다음 단계를 완료하십시오. 다음을 참조하십시오.

- "AWS에서 Cloud Volumes ONTAP 시작하기".
- "Cloud Manager를 사용하여 AWS에서 커넥터를 생성합니다"

단계

1. Cloud Manager에 자격 증명을 추가합니다.
2. 작업 영역을 만듭니다.
3. AWS용 커넥터를 추가합니다. AWS를 공급자로 선택합니다.
4. 클라우드 환경을 위한 작업 환경을 구축합니다.
    a. 위치: "AWS(Amazon Web Services)"
    b. 유형: "Cloud Volumes ONTAP HA"
5. OpenShift 클러스터를 가져옵니다. 클러스터가 방금 생성한 작업 환경에 연결됩니다.

a. NetApp 클러스터 세부 정보를 보려면 * K8s * > * 클러스터 목록 * > * 클러스터 세부 정보 * 를 선택합니다.

b. 오른쪽 위 모서리에서 Trident 버전을 확인합니다.

c. NetApp을 공급자 로 보여주는 Cloud Volumes ONTAP 클러스터 스토리지 클래스를 참조하십시오.

   그러면 Red Hat OpenShift 클러스터가 가져와 기본 스토리지 클래스가 할당됩니다. 스토리지 클래스를 선택합니다. Trident는 가져오기 및 검색 프로세스의 일부로 자동으로 설치됩니다.

6. 이 Cloud Volumes ONTAP 배포에서 모든 영구 볼륨 및 볼륨을 기록해 둡니다.

> Cloud Volumes ONTAP는 단일 노드 또는 고가용성으로 작동할 수 있습니다. HA가 활성화된 경우 AWS에서 실행 중인 HA 상태와 노드 구축 상태를 확인하십시오.

Astra Control Center를 설치합니다

표준을 따릅니다 "Astra Control Center 설치 지침".

> AWS는 일반 S3 버킷 유형을 사용합니다.

Google Cloud Platform에 **Astra Control Center**를 구축합니다

GCP(Google Cloud Platform) 퍼블릭 클라우드에서 호스팅되는 자가 관리형 Kubernetes 클러스터에 Astra Control Center를 구축할 수 있습니다.

GCP에 필요한 사항

GCP에 Astra Control Center를 구축하기 전에 다음 항목이 필요합니다.

- Astra Control Center 라이센스. 을 참조하십시오 "Astra Control Center 라이센스 요구 사항".
- "Astra Control Center 요구 사항을 충족합니다".
- NetApp Cloud Central 계정
- OCP를 사용하는 경우 Red Hat OpenShift Container Platform(OCP) 4.10
- OCP를 사용하는 경우 Red Hat OpenShift Container Platform(OCP) 권한(네임스페이스 수준에서 POD 생성)
- 버킷 및 커넥터를 생성할 수 있는 권한이 있는 GCP 서비스 계정

GCP의 운영 환경 요구 사항

> Astra Control Center를 호스팅하기 위해 선택한 운영 환경이 환경 공식 문서에 설명된 기본 리소스 요구 사항을 충족하는지 확인합니다.

Astra Control Center에는 환경의 리소스 요구 사항 외에 다음과 같은 리소스가 필요합니다.

구성 요소	요구 사항
백엔드 **NetApp Cloud Volumes ONTAP** 스토리지 용량입니다	최소 300GB가 사용 가능합니다
작업자 노드**(GCP** 컴퓨팅 요구사항**)**	총 3개 이상의 작업자 노드, vCPU 코어 4개, 12GB RAM

구성 요소	요구 사항
로드 밸런서	수신 트래픽을 운영 환경 클러스터의 서비스로 전송할 수 있도록 서비스 유형 "로드 밸런서"를 사용할 수 있습니다
FQDN(GCP DNS 영역**)**	Astra Control Center의 FQDN을 부하 분산 IP 주소로 가리키는 방법
Astra Trident(NetApp Cloud Manager에서 **Kubernetes** 클러스터 검색의 일부로 설치됨**)**	Astra Trident 21.04 이상 설치 및 구성, NetApp ONTAP 버전 9.5 이상 버전을 스토리지 백엔드로 사용합니다
이미지 레지스트리	Astra Control Center 빌드 이미지를 푸시할 수 있는 Google Container Registry와 같은 기존 개인 레지스트리가 있어야 합니다. 이미지를 업로드할 이미지 레지스트리의 URL을 제공해야 합니다. ⓘ 백업을 위해 Restic 이미지를 풀려면 익명 액세스를 설정해야 합니다.
Astra Trident/ONTAP 구성	Astra Control Center에서는 스토리지 클래스를 생성하고 기본 스토리지 클래스로 설정해야 합니다. Astra Control Center는 Kubernetes 클러스터를 NetApp Cloud Manager로 가져올 때 생성되는 다음과 같은 ONTAP Kubernetes 스토리지 클래스를 지원합니다. Astra Trident에서 제공합니다. • `vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-ha-san csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-san csi.trident.netapp.io`

ⓘ 이러한 요구 사항에서는 Astra Control Center가 운영 환경에서 실행되는 유일한 애플리케이션이라고 가정합니다. 환경에서 추가 애플리케이션이 실행 중인 경우 이러한 최소 요구 사항을 적절히 조정합니다.

GCP 구축 개요

다음은 Astra Control Center를 스토리지 백엔드로 Cloud Volumes ONTAP를 사용하는 GCP의 자체 관리 OCP 클러스터에 설치하는 프로세스의 개요입니다.

이러한 각 단계는 아래에 자세히 설명되어 있습니다.

1. GCP에 RedHat OpenShift 클러스터를 설치합니다.
2. GCP 프로젝트 및 가상 프라이빗 클라우드를 생성합니다.
3. IAM 권한이 충분한지 확인하십시오.
4. GCP를 구성합니다.

5. NetApp Cloud Manager 구성.
6. Astra Control Center를 설치하고 구성합니다.

GCP에 RedHat OpenShift 클러스터를 설치합니다

첫 번째 단계는 GCP에 RedHat OpenShift 클러스터를 설치하는 것입니다.

설치 지침은 다음을 참조하십시오.

- "GCP에서 OpenShift 클러스터 설치"
- "GCP 서비스 계정 생성"

GCP 프로젝트 및 가상 프라이빗 클라우드를 생성합니다

하나 이상의 GCP 프로젝트 및 VPC(가상 프라이빗 클라우드)를 생성합니다.

> OpenShift는 자체 리소스 그룹을 생성할 수 있습니다. 또한 GCP VPC를 정의해야 합니다. OpenShift 설명서를 참조하십시오.

플랫폼 클러스터 리소스 그룹과 대상 애플리케이션 OpenShift 클러스터 리소스 그룹을 생성할 수 있습니다.

IAM 권한이 충분한지 확인하십시오

RedHat OpenShift 클러스터와 NetApp Cloud Manager Connector를 설치할 수 있도록 충분한 IAM 역할 및 권한이 있는지 확인합니다.

을 참조하십시오 "초기 GCP 자격 증명 및 권한".

GCP를 구성합니다

그런 다음 VPC를 생성하고, 컴퓨팅 인스턴스를 설정하고, Google Cloud Object Storage를 생성하고, Google Container Register를 생성하여 Astra Control Center 이미지를 호스팅하고, 이미지를 이 레지스트리로 푸시하도록 GCP를 구성합니다.

GCP 문서에 따라 다음 단계를 완료합니다. GCP에서 OpenShift 클러스터 설치를 참조하십시오.

1. CVO 백엔드가 있는 OCP 클러스터에 사용할 GCP에서 사용할 GCP 프로젝트 및 VPC를 GCP에서 생성합니다.
2. 컴퓨팅 인스턴스를 검토합니다. GCP의 베어 메탈 서버 또는 VM이 될 수 있습니다.
3. 인스턴스 유형이 마스터 및 작업자 노드에 대한 Astra 최소 리소스 요구 사항과 일치하지 않으면 Astra 요구 사항을 충족하도록 GCP의 인스턴스 유형을 변경합니다. 을 참조하십시오 "Astra Control Center 요구 사항".
4. 백업을 저장할 하나 이상의 GCP Cloud Storage Bucket을 생성합니다.
5. 버킷 액세스에 필요한 암호를 생성합니다.
6. 모든 Astra Control Center 이미지를 호스트하기 위해 Google Container Registry를 생성합니다.
7. 모든 Astra Control Center 이미지에 대해 Docker 푸시/풀용 Google Container Registry 액세스를 설정합니다.

   예: 다음 스크립트를 입력하여 ACC 이미지를 이 레지스트리로 푸시할 수 있습니다.

```
gcloud auth activate-service-account <service account email address>
--key-file=<GCP Service Account JSON file>
```

이 스크립트에는 Astra Control Center 매니페스트 파일과 Google Image 레지스트리 위치가 필요합니다.

예:

```
manifestfile=astra-control-center-<version>.manifest
GCP_CR_REGISTRY=<target image repository>
ASTRA_REGISTRY=<source ACC image repository>

while IFS= read -r image; do
    echo "image: $ASTRA_REGISTRY/$image $GCP_CR_REGISTRY/$image"
    root_image=${image%:*}
    echo $root_image
    docker pull $ASTRA_REGISTRY/$image
    docker tag $ASTRA_REGISTRY/$image $GCP_CR_REGISTRY/$image
    docker push $GCP_CR_REGISTRY/$image
done < astra-control-center-22.04.41.manifest
```

8. DNS 존 설정

NetApp Cloud Manager 구성

Cloud Manager를 사용하여 작업 공간을 생성하고, GCP에 커넥터를 추가하고, 작업 환경을 생성하고, 클러스터를 가져옵니다.

Cloud Manager 설명서에 따라 다음 단계를 완료하십시오. 을 참조하십시오 "GCP에서 Cloud Volumes ONTAP 시작하기".

필요한 것

- 필요한 IAM 권한 및 역할을 사용하여 GCP 서비스 계정에 액세스합니다

단계

1. Cloud Manager에 자격 증명을 추가합니다. 을 참조하십시오 "GCP 계정 추가".
2. GCP용 커넥터를 추가합니다.
   a. 공급자로 "GCP"를 선택합니다.
   b. GCP 자격 증명을 입력합니다. 을 참조하십시오 "Cloud Manager에서 GCP에 커넥터 생성".
   c. 커넥터가 실행 중인지 확인하고 해당 커넥터로 전환합니다.
3. 클라우드 환경을 위한 작업 환경을 구축합니다.
   a. 위치:"GCP"
   b. 유형: "Cloud Volumes ONTAP HA"

4. OpenShift 클러스터를 가져옵니다. 클러스터가 방금 생성한 작업 환경에 연결됩니다.
   a. NetApp 클러스터 세부 정보를 보려면 * K8s * > * 클러스터 목록 * > * 클러스터 세부 정보 * 를 선택합니다.
   b. 오른쪽 위 모서리에서 Trident 버전을 확인합니다.
   c. "NetApp"을 프로비저닝자로 나타내는 Cloud Volumes ONTAP 클러스터 스토리지 클래스를 확인하십시오.

      그러면 Red Hat OpenShift 클러스터가 가져와 기본 스토리지 클래스가 할당됩니다. 스토리지 클래스를 선택합니다. Trident는 가져오기 및 검색 프로세스의 일부로 자동으로 설치됩니다.
5. 이 Cloud Volumes ONTAP 배포에서 모든 영구 볼륨 및 볼륨을 기록해 둡니다.

> Cloud Volumes ONTAP는 단일 노드 또는 고가용성(HA)으로 작동할 수 있습니다. HA가 사용되도록 설정된 경우 GCP에서 실행 중인 HA 상태 및 노드 배포 상태를 확인합니다.

Astra Control Center를 설치합니다

표준을 따릅니다 "Astra Control Center 설치 지침".

> GCP는 일반 S3 버킷 유형을 사용합니다.

1. Docker Secret를 생성하여 Astra Control Center 설치를 위한 이미지를 가져옵니다.

```
kubectl create secret docker-registry <secret name>
--docker-server=<Registry location>
--docker-username=_json_key
--docker-password="$(cat <GCP Service Account JSON file>)"
--namespace=pcloud
```

Microsoft Azure에 **Astra Control Center**를 구축합니다

Microsoft Azure 퍼블릭 클라우드에서 호스팅되는 자가 관리형 Kubernetes 클러스터에 Astra Control Center를 구축할 수 있습니다.

Azure에 필요한 기능

Azure에 Astra Control Center를 배포하기 전에 다음 항목이 필요합니다.

- Astra Control Center 라이센스. 을 참조하십시오 "Astra Control Center 라이센스 요구 사항".
- "Astra Control Center 요구 사항을 충족합니다".
- NetApp Cloud Central 계정
- OCP를 사용하는 경우 Red Hat OpenShift Container Platform(OCP) 4.8
- OCP를 사용하는 경우 Red Hat OpenShift Container Platform(OCP) 권한(네임스페이스 수준에서 POD 생성)
- 버킷 및 커넥터를 생성할 수 있는 권한이 있는 Azure 자격 증명

Azure의 운영 환경 요구사항

Astra Control Center를 호스팅하기 위해 선택한 운영 환경이 환경 공식 문서에 설명된 기본 리소스 요구 사항을 충족하는지 확인합니다.

Astra Control Center에는 환경의 리소스 요구 사항 외에 다음과 같은 리소스가 필요합니다.

을 참조하십시오 "Astra Control Center 운영 환경 요구 사항".

구성 요소	요구 사항
백엔드 **NetApp Cloud Volumes ONTAP** 스토리지 용량입니다	최소 300GB가 사용 가능합니다
작업자 노드**(Azure** 컴퓨팅 요구 사항**)**	총 3개 이상의 작업자 노드, vCPU 코어 4개, 12GB RAM
로드 밸런서	수신 트래픽을 운영 환경 클러스터의 서비스로 전송할 수 있도록 서비스 유형 "로드 밸런서"를 사용할 수 있습니다
FQDN(Azure DNS 영역**)**	Astra Control Center의 FQDN을 부하 분산 IP 주소로 가리키는 방법
Astra Trident(NetApp Cloud Manager에서 **Kubernetes** 클러스터 검색의 일부로 설치됨**)**	설치 및 구성된 Astra Trident 21.04 이상 및 NetApp ONTAP 버전 9.5 이상이 스토리지 백엔드로 사용됩니다
이미지 레지스트리	Astra Control Center 빌드 이미지를 푸시할 수 있는 Azure 컨테이너 레지스트리(ACR)와 같은 기존 개인 레지스트리가 있어야 합니다. 이미지를 업로드할 이미지 레지스트리의 URL을 제공해야 합니다. ⓘ 백업을 위해 Restic 이미지를 풀려면 익명 액세스를 설정해야 합니다.
Astra Trident/ONTAP 구성	Astra Control Center에서는 스토리지 클래스를 생성하고 기본 스토리지 클래스로 설정해야 합니다. Astra Control Center는 Kubernetes 클러스터를 NetApp Cloud Manager로 가져올 때 생성되는 다음과 같은 ONTAP Kubernetes 스토리지 클래스를 지원합니다. Astra Trident에서 제공합니다. • `vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-ha-san csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-san csi.trident.netapp.io`

ⓘ 이러한 요구 사항에서는 Astra Control Center가 운영 환경에서 실행되는 유일한 애플리케이션이라고 가정합니다. 환경에서 추가 애플리케이션이 실행 중인 경우 이러한 최소 요구 사항을 적절히 조정합니다.

Azure 구축 개요

다음은 Azure용 Astra Control Center를 설치하는 프로세스의 개요입니다.

이러한 각 단계는 아래에 자세히 설명되어 있습니다.

1. Azure에 RedHat OpenShift 클러스터를 설치합니다.
2. Azure 리소스 그룹을 생성합니다.
3. IAM 권한이 충분한지 확인하십시오.
4. Azure를 구성합니다.
5. NetApp Cloud Manager 구성.
6. Astra Control Center를 설치하고 구성합니다.

Azure에 RedHat OpenShift 클러스터를 설치합니다

첫 번째 단계는 Azure에 RedHat OpenShift 클러스터를 설치하는 것입니다.

설치 지침은 의 RedHat 설명서를 참조하십시오 "Azure에 OpenShift 클러스터 설치" 및 "Azure 계정을 설치하는 중입니다".

Azure 리소스 그룹을 생성합니다

Azure 리소스 그룹을 하나 이상 생성합니다.

> OpenShift는 자체 리소스 그룹을 생성할 수 있습니다. 또한 Azure 리소스 그룹을 정의해야 합니다. OpenShift 설명서를 참조하십시오.

플랫폼 클러스터 리소스 그룹과 대상 애플리케이션 OpenShift 클러스터 리소스 그룹을 생성할 수 있습니다.

IAM 권한이 충분한지 확인하십시오

RedHat OpenShift 클러스터와 NetApp Cloud Manager Connector를 설치할 수 있도록 충분한 IAM 역할 및 권한이 있는지 확인합니다.

을 참조하십시오 "Azure 자격 증명 및 권한".

Azure를 구성합니다

그런 다음 가상 네트워크를 만들고, 컴퓨팅 인스턴스를 설정하고, Azure Blob 컨테이너를 만들고, Astra Control Center 이미지를 호스팅하기 위해 ACR(Azure Container Register)을 만들고, 이 레지스트리로 이미지를 푸시하도록 Azure를 구성합니다.

Azure 설명서에 따라 다음 단계를 완료합니다. 을 참조하십시오 "Azure에 OpenShift 클러스터 설치".

1. Azure 가상 네트워크를 생성합니다.
2. 컴퓨팅 인스턴스를 검토합니다. Azure의 베어 메탈 서버 또는 VM이 될 수 있습니다.
3. 인스턴스 유형이 마스터 및 작업자 노드에 대한 Astra 최소 리소스 요구 사항과 일치하지 않으면 Azure의 인스턴스 유형을 Astra 요구 사항에 맞게 변경합니다. 을 참조하십시오 "Astra Control Center 요구 사항".

4. 백업을 저장할 Azure Blob 컨테이너를 하나 이상 생성합니다.
5. 저장소 계정을 생성합니다. Astra Control Center에서 버킷으로 사용할 컨테이너를 생성하려면 저장소 계정이 필요합니다.
6. 버킷 액세스에 필요한 암호를 생성합니다.
7. Azure Container Registry(ACR)를 생성하여 모든 Astra Control Center 이미지를 호스트합니다.
8. Docker에 대한 ACR 액세스를 설정하여 모든 Astra Control Center 이미지를 푸시/풀합니다.
9. 다음 스크립트를 입력하여 ACC 이미지를 이 레지스트리에 푸시합니다.

```
az acr login -n <AZ ACR URL/Location>
This script requires ACC manifest file and your Azure ACR location.
```

   - 예 *:

```
manifestfile=astra-control-center-<version>.manifest
AZ_ACR_REGISTRY=<target image repository>
ASTRA_REGISTRY=<source ACC image repository>

while IFS= read -r image; do
    echo "image: $ASTRA_REGISTRY/$image $AZ_ACR_REGISTRY/$image"
    root_image=${image%:*}
    echo $root_image
    docker pull $ASTRA_REGISTRY/$image
    docker tag $ASTRA_REGISTRY/$image $AZ_ACR_REGISTRYY/$image
    docker push $AZ_ACR_REGISTRY/$image
done < astra-control-center-22.04.41.manifest
```

10. DNS 존 설정

NetApp Cloud Manager 구성

Cloud Manager를 사용하여 작업 영역을 만들고, Azure에 커넥터를 추가하고, 작업 환경을 생성하고, 클러스터를 가져옵니다.

Cloud Manager 설명서에 따라 다음 단계를 완료하십시오. 을 참조하십시오 "Azure에서 Cloud Manager 시작하기".

필요한 것

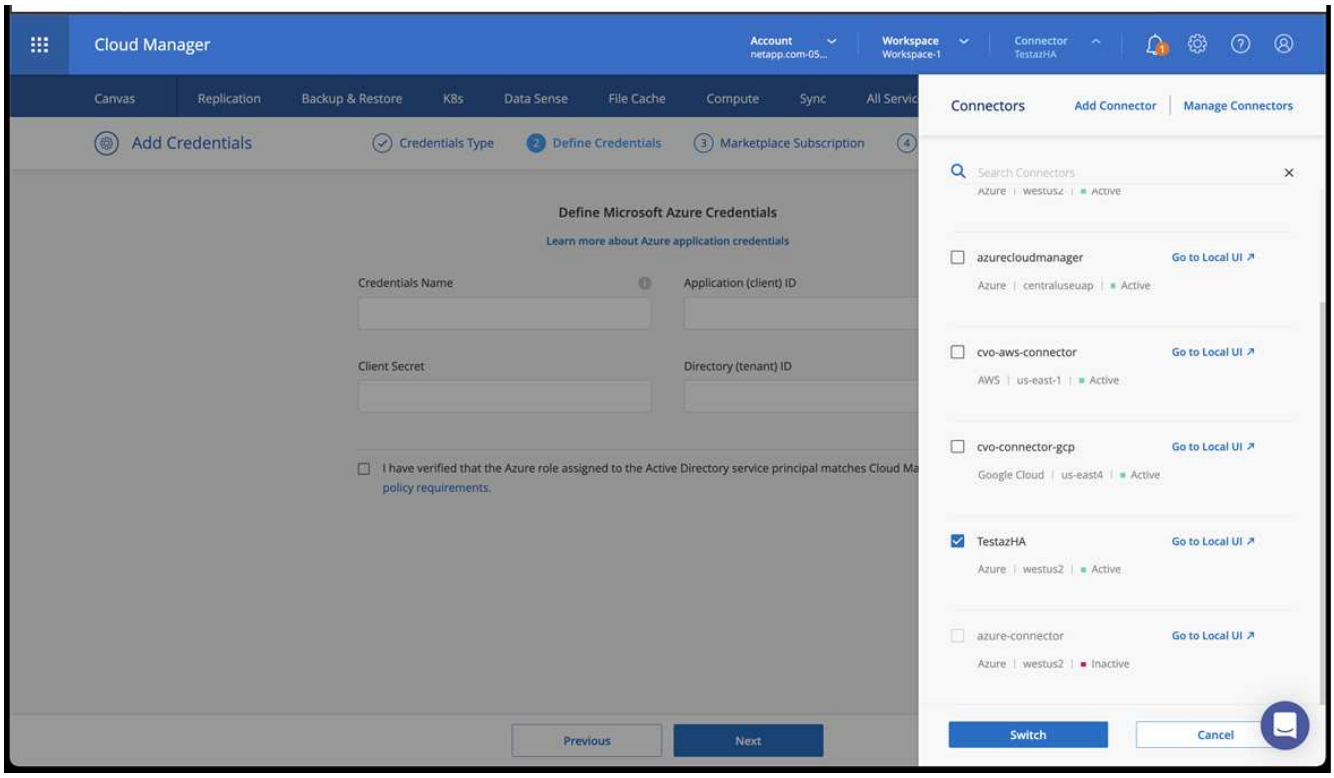
필요한 IAM 권한 및 역할을 사용하여 Azure 계정에 액세스합니다

단계

1. Cloud Manager에 자격 증명을 추가합니다.
2. Azure용 커넥터를 추가합니다. 을 참조하십시오 "Cloud Manager 정책".
   a. 공급자로 * Azure * 를 선택합니다.
   b. 애플리케이션 ID, 클라이언트 암호 및 디렉토리(테넌트) ID를 비롯한 Azure 자격 증명을 입력합니다.

을 참조하십시오 "Cloud Manager에서 Azure에 커넥터 만들기".

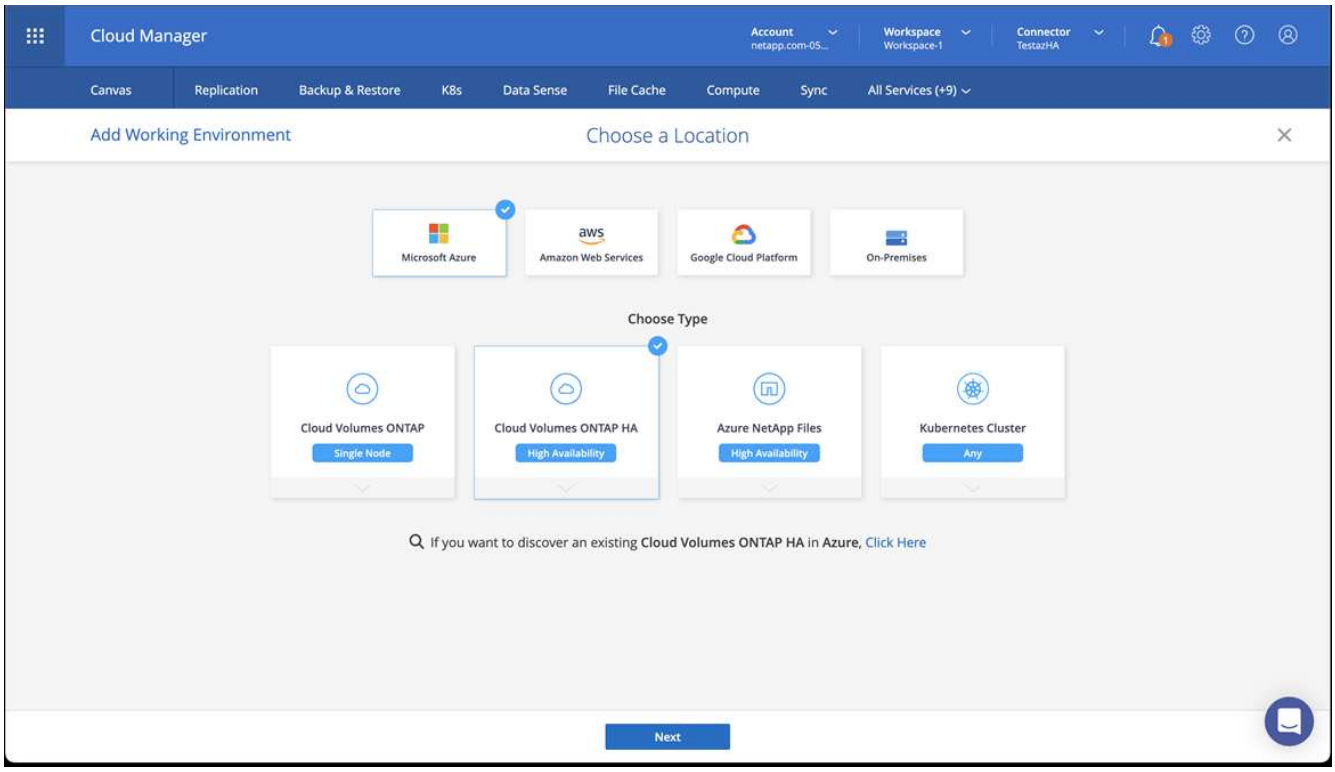
3. 커넥터가 실행 중인지 확인하고 해당 커넥터로 전환합니다.



4. 클라우드 환경을 위한 작업 환경을 구축합니다.

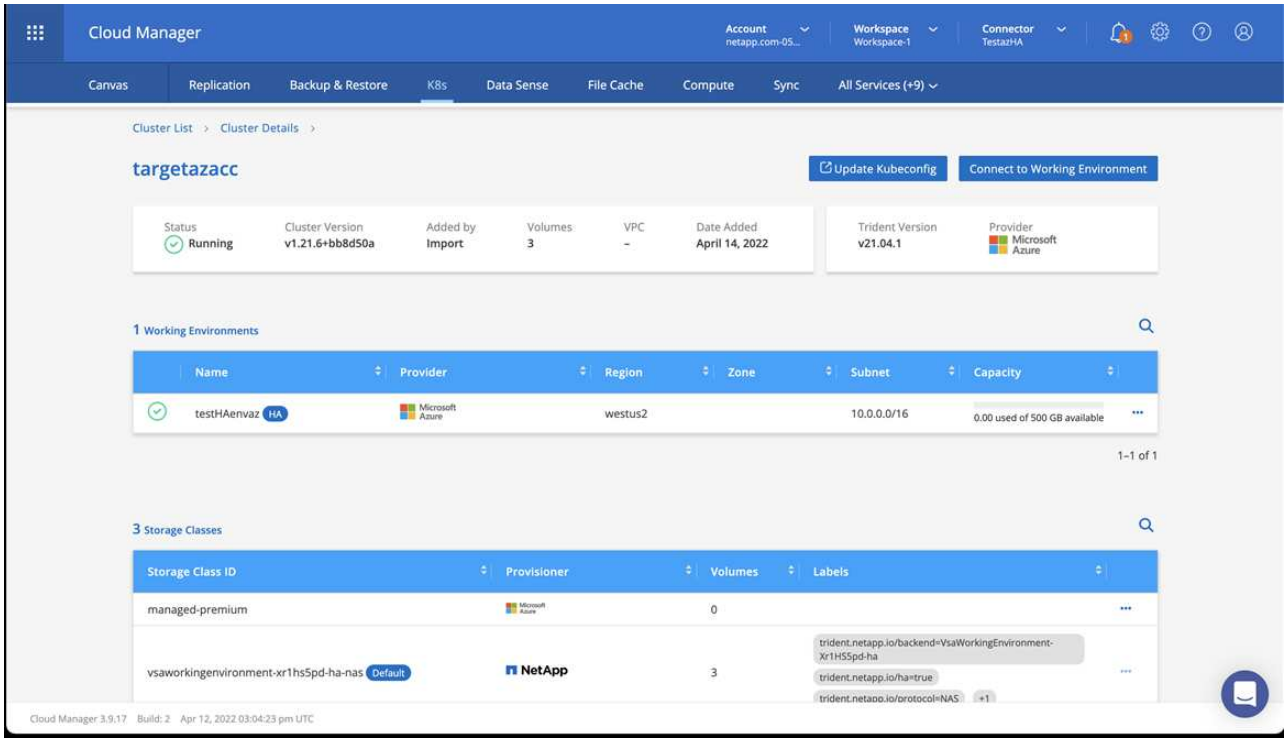
   a. 위치: "Microsoft Azure".

   b. "Cloud Volumes ONTAP HA"를 입력합니다.



5. OpenShift 클러스터를 가져옵니다. 클러스터가 방금 생성한 작업 환경에 연결됩니다.

   a. NetApp 클러스터 세부 정보를 보려면 * K8s * > * 클러스터 목록 * > * 클러스터 세부 정보 * 를 선택합니다.



   b. 오른쪽 위 모서리에서 Trident 버전을 확인합니다.

   c. NetApp을 공급자 로 보여주는 Cloud Volumes ONTAP 클러스터 스토리지 클래스를 참조하십시오.

이렇게 하면 Red Hat OpenShift 클러스터를 가져오고 기본 스토리지 클래스를 할당합니다. 스토리지 클래스를

선택합니다. Trident는 가져오기 및 검색 프로세스의 일부로 자동으로 설치됩니다.

6. 이 Cloud Volumes ONTAP 배포에서 모든 영구 볼륨 및 볼륨을 기록해 둡니다.
7. Cloud Volumes ONTAP는 단일 노드 또는 고가용성으로 작동할 수 있습니다. HA가 활성화된 경우 Azure에서 실행 중인 HA 상태와 노드 배포 상태를 확인하십시오.

Astra Control Center를 설치하고 구성합니다

Astra Control Center를 표준으로 설치합니다 "설치 지침".

Astra Control Center를 사용하여 Azure 버킷을 추가합니다. 을 참조하십시오 "Astra Control Center를 설정하고 버킷을 추가합니다".

Astra Control Center를 설정합니다

Astra Control Center는 스토리지 백엔드로 ONTAP 및 Astra 데이터 저장소를 지원 및 모니터링합니다. Astra Control Center를 설치하고, UI에 로그인하고, 암호를 변경하면 라이센스를 설정하고, 클러스터를 추가하고, 스토리지를 관리하고, 버킷을 추가할 수 있습니다.

작업

- Astra Control Center에 대한 라이센스를 추가합니다
- 클러스터 추가
- 스토리지 백엔드를 추가합니다
- 버킷을 추가합니다

Astra Control Center에 대한 라이센스를 추가합니다

UI 또는 를 사용하여 새 라이센스를 추가할 수 있습니다 "API를 참조하십시오" Astra Control Center의 모든 기능을 활용할 수 있습니다. 라이센스가 없으면 Astra Control Center의 사용은 사용자 관리 및 새 클러스터 추가로 제한됩니다.

라이선스 계산 방법에 대한 자세한 내용은 을 참조하십시오 "라이센싱".

> 기존 평가판 또는 전체 라이센스를 업데이트하려면 을 참조하십시오 "기존 라이센스를 업데이트합니다".

Astra Control Center 라이센스는 Kubernetes CPU 장치를 사용하여 CPU 리소스를 측정합니다. 라이센스는 모든 관리되는 Kubernetes 클러스터의 작업자 노드에 할당된 CPU 리소스를 고려해야 합니다. 라이센스를 추가하기 전에 에서 라이센스 파일(NLF)을 얻어야 합니다 "NetApp Support 사이트".

또한 평가판 라이센스가 있는 Astra Control Center를 사용하여 라이센스를 다운로드한 날짜로부터 90일 동안 Astra Control Center를 사용할 수 있습니다. 등록하면 무료 평가판을 사용할 수 있습니다 "여기".

> 설치가 라이센스 CPU 유닛 수를 초과하여 증가할 경우, Astra Control Center를 통해 새 애플리케이션을 관리할 수 없습니다. 용량이 초과되면 경고가 표시됩니다.

필요한 것

에서 Astra Control Center를 다운로드한 경우 "NetApp Support 사이트"또한 NetApp 라이센스 파일(NLF)도 다운로드했습니다. 이 라이센스 파일에 대한 액세스 권한이 있는지 확인하십시오.

단계

1. Astra Control Center UI에 로그인합니다.
2. 계정 * > * 라이센스 * 를 선택합니다.
3. 라이센스 추가 * 를 선택합니다.
4. 다운로드한 라이센스 파일(NLF)으로 이동합니다.
5. 라이센스 추가 * 를 선택합니다.

계정 * > * 라이센스 * 페이지에는 라이센스 정보, 만료 날짜, 라이센스 일련 번호, 계정 ID 및 사용된 CPU 단위가 표시됩니다.

평가 라이센스가 있는 경우 ASUP를 보내지 않을 경우 Astra Control Center에 장애가 발생할 경우 데이터 손실을 방지하기 위해 계정 ID를 저장해야 합니다.

클러스터 추가

앱 관리를 시작하려면 Kubernetes 클러스터를 추가하고 이를 컴퓨팅 리소스로 관리합니다. Kubernetes 애플리케이션을 검색하려면 Astra Control Center용 클러스터를 추가해야 합니다. Astra Data Store의 경우, Astra Data Store에서 프로비저닝한 볼륨을 사용하는 애플리케이션이 포함된 Kubernetes 앱 클러스터를 추가하려고 합니다.

관리를 위해 Astra Control Center에 다른 클러스터를 추가하기 전에 먼저 Astra Control Center에서 클러스터를 관리하는 것이 좋습니다. 메트릭 및 문제 해결을 위해 Kubemetrics 데이터 및 클러스터 관련 데이터를 전송하려면 관리 중인 초기 클러스터가 필요합니다. 클러스터 추가 * 기능을 사용하여 Astra Control Center로 클러스터를 관리할 수 있습니다.

Astra Control이 클러스터를 관리할 때 클러스터의 기본 스토리지 클래스를 추적합니다. 를 사용하여 스토리지 클래스를 변경하는 경우 `kubectl` 명령, Astra Control은 변경 사항을 되돌립니다. Astra Control에서 관리하는 클러스터의 기본 스토리지 클래스를 변경하려면 다음 방법 중 하나를 사용하십시오.

- Astra Control API를 사용합니다 `PUT /managedClusters` 를 사용하여 다른 기본 스토리지 클래스를 할당합니다 `DefaultStorageClass` 매개 변수.
- Astra Control 웹 UI를 사용하여 다른 기본 스토리지 클래스를 할당합니다. 을 참조하십시오 기본 스토리지 클래스를 변경합니다.

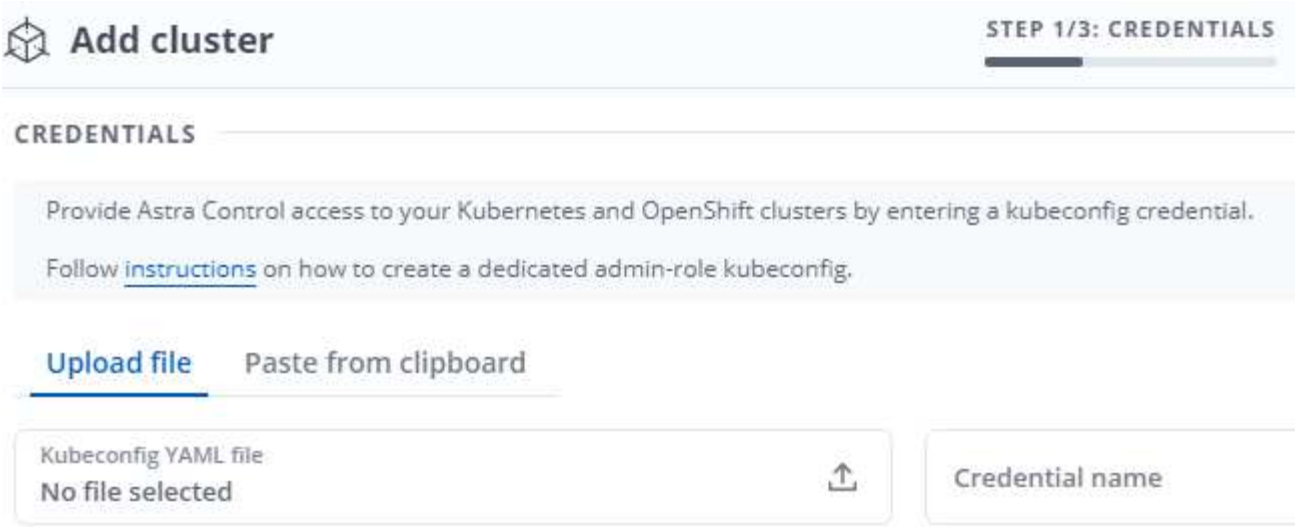
필요한 것

- 클러스터를 추가하기 전에 필요한 를 검토 및 수행합니다 "선행 작업".

단계

1. Astra Control Center UI의 * Dashboard * 에서 Clusters 섹션에서 * Add * 를 선택합니다.
2. 열리는 * Add Cluster * (클러스터 추가 *) 창에서 를 업로드합니다 `kubeconfig.yaml` 의 내용을 파일 또는 붙여 넣습니다 `kubeconfig.yaml` 파일.

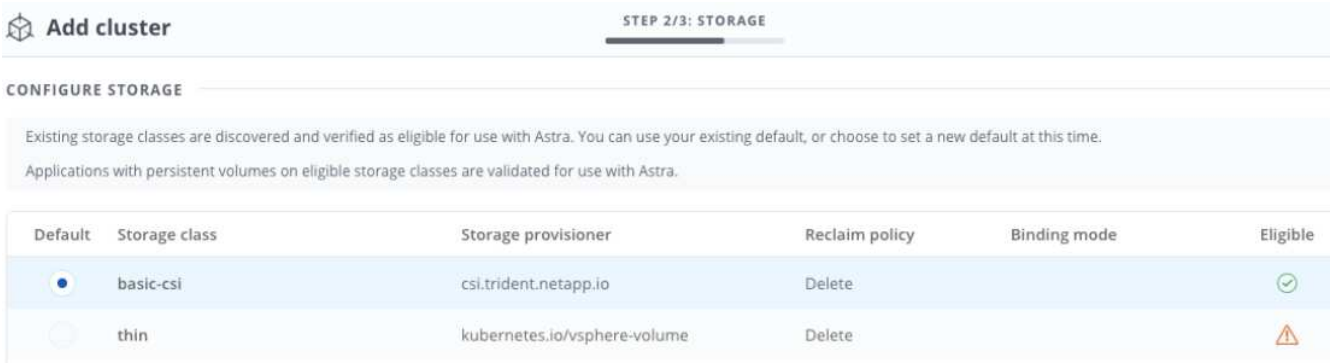
   를 클릭합니다 `kubeconfig.yaml` 파일에는 클러스터 자격 증명 1개에 대한 * 만 포함되어야 합니다 *.



> 직접 만드는 경우 `kubeconfig` 파일에서 * 하나의 * 컨텍스트 요소만 정의해야 합니다. 을 참조하십시오 "Kubernetes 문서" 을 참조하십시오 `kubeconfig` 파일.

3. 자격 증명 이름을 제공하십시오. 기본적으로 자격 증명 이름은 클러스터 이름으로 자동 채워집니다.
4. 스토리지 구성 * 을 선택합니다.
5. 이 Kubernetes 클러스터에 사용할 스토리지 클래스를 선택하고 * Review * 를 선택하십시오.

> ONTAP 스토리지 또는 Astra 데이터 저장소에서 지원하는 Trident 스토리지 클래스를 선택해야 합니다.



6. 정보를 검토하고 모든 내용이 양호하면 * 클러스터 추가 * 를 선택합니다.

결과

클러스터가 * 검색 * 상태로 전환되고 * 실행 * 으로 변경됩니다. Kubernetes 클러스터를 성공적으로 추가했으며 현재 Astra Control Center에서 관리하고 있습니다.

> Astra Control Center에서 관리할 클러스터를 추가한 후 모니터링 연산자를 구축하는 데 몇 분이 걸릴 수 있습니다. 그 전까지는 알림 아이콘이 빨간색으로 바뀌고 * 모니터링 에이전트 상태 확인 실패 * 이벤트를 기록합니다. Astra Control Center가 올바른 상태를 획득하면 문제가 해결되므로 이 문제를 무시할 수 있습니다. 몇 분 이내에 문제가 해결되지 않으면 클러스터로 이동하여 를 실행합니다 `oc get pods -n netapp-monitoring` 시작점으로 사용됩니다. 문제를 디버깅하려면 모니터링 운영자 로그를 확인해야 합니다.

스토리지 백엔드를 추가합니다

Astra Control에서 리소스를 관리할 수 있도록 스토리지 백엔드를 추가할 수 있습니다. 관리되는 클러스터에 스토리지 백엔드를 구축하거나 기존 스토리지 백엔드를 사용할 수 있습니다.

Astra Control에서 스토리지 클러스터를 스토리지 백엔드로 관리하면 PVS(영구적 볼륨)와 스토리지 백엔드 간의 연결 및 추가 스토리지 메트릭을 얻을 수 있습니다.

기존 **Astra Data Store** 구축에 필요한 사항

- Kubernetes 앱 클러스터와 기본 컴퓨팅 클러스터가 추가되었습니다.

> Astra Data Store용 Kubernetes 앱 클러스터를 추가하고 Astra Control에서 관리하는 경우 클러스터가 로 표시됩니다 `unmanaged` 을 클릭합니다. 다음으로 Astra Data Store가 포함된 컴퓨팅 클러스터를 추가하고 Kubernetes 애플리케이션 클러스터를 포함해야 합니다. UI의 * backends * 에서 이 작업을 수행할 수 있습니다. 클러스터의 Actions 메뉴를 선택하고 를 선택합니다 `Manage`, 및 "클러스터를 추가합니다". 클러스터 상태 후 `unmanaged` Kubernetes 클러스터 이름이 변경되면 백엔드를 추가하는 작업을 계속 진행할 수 있습니다.

새로운 **Astra Data Store** 구축에 필요한 사항

- 있습니다 "배포하려는 설치 번들 버전을 업로드했습니다" Astra Control에 액세스할 수 있는 위치
- 배포에 사용할 Kubernetes 클러스터를 추가했습니다.
- 을(를) 업로드했습니다 Astra Data Store 라이센스 Astra Control에 액세스할 수 있는 위치에 배포할 수 있습니다.

옵션

- 스토리지 리소스 구축
- 기존 스토리지 백엔드를 사용합니다

스토리지 리소스 구축

새로운 Astra Data Store를 구축하고 관련 스토리지 백엔드를 관리할 수 있습니다.

단계

1. 대시보드 또는 백엔드 메뉴에서 이동합니다.
   - 대시보드 * 에서: 리소스 요약의 스토리지 백엔드 창에서 링크를 선택하고 백엔드 섹션에서 * 추가 * 를 선택합니다.
   - 시작 * 백엔드 *:
     i. 왼쪽 탐색 영역에서 * backends * 를 선택합니다.
     ii. 추가 * 를 선택합니다.
2. 배포 * 탭에서 * Astra Data Store * 배포 옵션을 선택합니다.
3. 배포할 Astra Data Store 패키지를 선택합니다.
   a. Astra Data Store 애플리케이션의 이름을 입력합니다.
   b. 배포할 Astra Data Store의 버전을 선택합니다.

> 배포하려는 버전을 아직 업로드하지 않은 경우 * 패키지 추가 * 옵션을 사용하거나 마법사를 종료하고 를 사용할 수 있습니다 "패키지 관리" 를 눌러 설치 번들을 업로드합니다.

4. 이전에 업로드한 Astra Data Store 라이센스를 선택하거나 * Add license * 옵션을 사용하여 응용 프로그램에 사용할 라이센스를 업로드합니다.

> 모든 권한이 있는 Astra Data Store 라이센스가 Kubernetes 클러스터와 연결되어 있으며, 이와 관련된 클러스터가 자동으로 표시됩니다. 관리되는 클러스터가 없는 경우 * 클러스터 추가 * 옵션을 선택하여 Astra Control 관리에 클러스터를 추가할 수 있습니다. Astra Data Store 라이센스의 경우 라이센스와 클러스터 간에 연결이 되지 않은 경우 마법사의 다음 페이지에서 이 연결을 정의할 수 있습니다.

5. Kubernetes 클러스터를 Astra Control 관리에 추가하지 않은 경우 * Kubernetes 클러스터 * 페이지에서 추가해야 합니다. 목록에서 기존 클러스터를 선택하거나 * 기본 클러스터 추가 * 를 선택하여 Astra Control 관리에 클러스터를 추가합니다.
6. Astra Data Store에 리소스를 제공할 Kubernetes 클러스터의 템플릿 크기를 선택합니다. 다음 중 하나를 선택할 수 있습니다.
   - 선택하십시오 `Recommended Kubernetes worker node requirements`에서 라이센스에 허용되는 내용에 따라 큰 서식 파일에서 작은 서식 파일을 선택합니다.
   - 선택하십시오 `Custom Kubernetes worker node requirements`에서 각 클러스터 노드에 대해 원하는 코어 수와 총 메모리를 선택합니다. 또한 코어 및 메모리에 대한 선택 기준을 충족하는 클러스터에 있는 노드의 수를 표시할 수도 있습니다.

> 템플릿을 선택할 때 더 큰 워크로드를 위해 더 많은 메모리와 코어를 가진 더 큰 노드를 선택하거나 더 작은 워크로드의 경우 더 많은 노드를 선택합니다. 라이센스에 허용되는 내용에 따라 템플릿을 선택해야 합니다. 권장되는 각 템플릿 옵션은 각 노드의 메모리 및 코어, 용량에 대한 템플릿 패턴을 충족하는 적합한 노드 수를 제안합니다.

7. 노드 구성:
   a. 노드 레이블을 추가하여 이 Astra Data Store 클러스터를 지원하는 작업자 노드 풀을 식별합니다.

> 구축 또는 구축을 시작하기 전에 Astra Data Store 구축에 사용할 클러스터의 각 개별 노드에 레이블을 추가해야 합니다.

   b. 노드당 용량(GiB)을 수동으로 구성하거나 허용되는 최대 노드 용량을 선택합니다.
   c. 클러스터에서 허용되는 최대 노드 수를 구성하거나 클러스터에서 최대 노드 수를 허용합니다.
8. (Astra Data Store 전체 라이센스만 해당) 보호 도메인에 사용할 레이블의 키를 입력합니다.

> 각 노드에 대해 키에 대한 고유 레이블을 3개 이상 생성합니다. 예를 들어, 키가 인 경우 `astra.datastore.protection.domain`다음과 같은 레이블을 만들 수 있습니다. `astra.datastore.protection.domain=domain1`,`astra.datastore.protection.domain=domain2`, 및 `astra.datastore.protection.domain=domain3`.

9. 관리 네트워크 구성:
   a. 작업자 노드 IP 주소와 동일한 서브넷에 있는 Astra Data Store 내부 관리에 대한 관리 IP 주소를 입력합니다.
   b. 관리 및 데이터 네트워크 모두에 동일한 NIC를 사용하거나 별도로 구성합니다.

c. 스토리지 액세스를 위한 데이터 네트워크 IP 주소 풀, 서브넷 마스크 및 게이트웨이를 입력합니다.

10. 구성을 검토하고 * deploy * 를 선택하여 설치를 시작합니다.

결과

설치가 완료되면 백엔드가 에 나타납니다 `available` 활성 성능 정보와 함께 백엔드 목록의 상태입니다.

> 백엔드가 표시되도록 페이지를 새로 고쳐야 할 수 있습니다.

기존 스토리지 백엔드를 사용합니다

검색된 ONTAP 또는 Astra Data Store 스토리지 백엔드를 Astra Control Center 관리 센터에 가져올 수 있습니다.

단계

1. 대시보드 또는 백엔드 메뉴에서 이동합니다.
   - 대시보드 * 에서: 리소스 요약의 스토리지 백엔드 창에서 링크를 선택하고 백엔드 섹션에서 * 추가 * 를 선택합니다.
   - 시작 * 백엔드 *:
     i. 왼쪽 탐색 영역에서 * backends * 를 선택합니다.
     ii. 관리되는 클러스터에서 검색된 백엔드에서 * 관리 * 를 선택하거나 * 추가 * 를 선택하여 기존 백엔드를 추가로 관리합니다.
2. 기존 * 사용 탭을 선택합니다.
3. 백엔드 유형에 따라 다음 중 하나를 수행합니다.
   - * Astra 데이터 저장소 *:
     i. Astra Data Store * 를 선택합니다.
     ii. 관리되는 컴퓨팅 클러스터를 선택하고 * Next * 를 선택합니다.
     iii. 백엔드 세부 정보를 확인하고 * Add storage backend * 를 선택합니다.
   - * ONTAP *:
     i. ONTAP * 를 선택하고 * Next * 를 선택합니다.
     ii. ONTAP 클러스터 관리 IP 주소 및 관리 자격 증명을 입력합니다.

     > 여기에 자격 증명을 입력한 사용자에게는 가 있어야 합니다 `ontapi` ONTAP 클러스터의 ONTAP System Manager에서 활성화된 사용자 로그인 액세스 방법입니다. SnapMirror 복제를 사용하려는 경우 액세스 방법을 설정합니다 `ontapi` 및 `http` 두 ONTAP 클러스터 모두에 있는 사용자의 경우. 을 참조하십시오 "사용자 계정 관리" 를 참조하십시오.

     iii. Review * 를 선택합니다.
     iv. 백엔드 세부 정보를 확인하고 * Add storage backend * 를 선택합니다.

결과

백엔드가 에 나타납니다 `available` 목록의 상태로 요약 정보를 표시합니다.

> 백엔드가 표시되도록 페이지를 새로 고쳐야 할 수 있습니다.

버킷을 추가합니다

애플리케이션과 영구 스토리지를 백업하려는 경우나 클러스터 간에 애플리케이션을 클론 복제하려는 경우에는 오브젝트 저장소 버킷 공급자를 추가하는 것이 중요합니다. Astra Control은 이러한 백업 또는 클론을 정의한 오브젝트 저장소 버킷에 저장합니다.

버킷을 추가하면 Astra Control은 하나의 버킷을 기본 버킷 표시기로 표시합니다. 사용자가 만든 첫 번째 버킷이 기본 버킷이 됩니다.

애플리케이션 구성과 영구 스토리지를 동일한 클러스터에 클론 복제할 경우 버킷이 필요하지 않습니다.

다음 버킷 유형 중 하나를 사용하십시오.

- NetApp ONTAP S3
- NetApp StorageGRID S3
- 일반 S3

> AWS(Amazon Web Services) 및 GCP(Google Cloud Platform)는 일반 S3 버킷 유형을 사용합니다.

- Microsoft Azure를 참조하십시오

> Astra Control Center는 Amazon S3를 일반 S3 버킷 공급자로 지원하지만, Astra Control Center는 Amazon의 S3 지원을 주장하는 모든 오브젝트 저장소 공급업체를 지원하지 않을 수 있습니다.

- Microsoft Azure를 참조하십시오

Astra Control API를 사용하여 버킷을 추가하는 방법에 대한 지침은 를 참조하십시오 "Astra 자동화 및 API 정보".

단계

1. 왼쪽 탐색 영역에서 * Bucket * 을 선택합니다.
   a. 추가 * 를 선택합니다.
   b. 버킷 유형을 선택합니다.

   > 버킷을 추가할 때 올바른 버킷 공급자를 선택하고 해당 공급자에 적합한 자격 증명을 제공합니다. 예를 들어, UI에서 NetApp ONTAP S3를 유형으로 받아들이고 StorageGRID 자격 증명을 받아들이지만, 이 버킷을 사용한 이후의 모든 애플리케이션 백업 및 복원이 실패합니다.

   c. 새 버킷 이름을 생성하거나 기존 버킷 이름과 선택적 설명을 입력합니다.

   > 버킷 이름 및 설명은 백업을 생성할 때 나중에 선택할 수 있는 백업 위치로 나타납니다. 이 이름은 보호 정책 구성 중에도 표시됩니다.

   d. S3 엔드포인트의 이름 또는 IP 주소를 입력합니다.
   e. 이 버킷을 모든 백업의 기본 버킷으로 사용하려면 를 선택합니다 `Make this bucket the default bucket for this private cloud` 옵션을 선택합니다.

> 이 옵션은 사용자가 만든 첫 번째 버킷에는 나타나지 않습니다.

f. 를 추가하여 계속합니다 자격 증명 정보.

S3 액세스 자격 증명을 추가합니다

언제든지 S3 액세스 자격 증명을 추가할 수 있습니다.

단계

1. Bucket 대화상자에서 * Add * 또는 * Use Existing * 탭을 선택합니다.
   a. Astra Control의 다른 자격 증명과 구별되는 자격 증명의 이름을 입력합니다.
   b. 클립보드의 내용을 붙여 넣어 액세스 ID와 비밀 키를 입력합니다.

기본 스토리지 클래스를 변경합니다

클러스터의 기본 스토리지 클래스를 변경할 수 있습니다.

단계

1. Astra Control Center 웹 UI에서 * Clusters * 를 선택합니다.
2. 클러스터 * 페이지에서 변경할 클러스터를 선택합니다.
3. Storage * 탭을 선택합니다.
4. 스토리지 클래스 * 범주를 선택합니다.
5. 기본값으로 설정할 스토리지 클래스에 대해 * Actions * 메뉴를 선택합니다.
6. Set as default * 를 선택합니다.

다음 단계

Astra Control Center에 로그인하고 클러스터를 추가했으므로 이제 Astra Control Center의 애플리케이션 데이터 관리 기능을 사용할 준비가 되었습니다.

- "사용자 관리"
- "앱 관리를 시작합니다"
- "앱 보호"
- "앱 클론 복제"
- "알림을 관리합니다"
- "Cloud Insights에 연결합니다"
- "사용자 지정 TLS 인증서를 추가합니다"

자세한 내용을 확인하십시오

- "Astra Control API를 사용합니다"
- "알려진 문제"

클러스터 추가를 위한 사전 요구사항

클러스터를 추가하기 전에 사전 요구 조건이 충족되는지 확인해야 합니다. 또한 자격 검사를 실행하여 클러스터를 Astra Control Center에 추가할 준비가 되었는지 확인해야 합니다.

클러스터를 추가하기 전에 필요한 사항

클러스터가 에 나와 있는 요구 사항을 충족하는지 확인합니다 "애플리케이션 클러스터 요구사항".

> 관리되는 컴퓨팅 리소스로 두 번째 OpenShift 4.6, 4.7 또는 4.8 클러스터를 추가하려는 경우 Astra Trident Volume Snapshot 기능이 활성화되어 있는지 확인해야 합니다. 공식 Astra Trident를 참조하십시오 "지침" Astra Trident를 사용하여 볼륨 스냅샷을 활성화하고 테스트합니다.

- A로 구성된 Astra Trident StorageClasses "지원되는 스토리지 백엔드" (모든 유형의 클러스터에 필요)
- Astra Control Center를 사용하여 앱을 백업 및 복원하기 위해 백업 ONTAP 시스템에 설정된 고급 사용자 및 사용자 ID입니다. ONTAP 명령줄에서 다음 명령을 실행합니다.
  `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -superuser sysm --anon 65534`
- Astra Trident `volumesnapshotclass` 관리자가 정의한 개체입니다. Astra Trident를 참조하십시오 "지침" Astra Trident를 사용하여 볼륨 스냅샷을 활성화하고 테스트합니다.
- Kubernetes 클러스터에 대해 단일 기본 스토리지 클래스만 정의되어 있는지 확인하십시오.

자격 검사를 실행합니다

다음 자격 검사를 실행하여 클러스터를 Astra Control Center에 추가할 준비가 되었는지 확인합니다.

단계

1. Trident 버전을 확인합니다.

   ```
   kubectl get tridentversions -n trident
   ```

   Trident가 있으면 다음과 유사한 출력이 표시됩니다.

   ```
   NAME       VERSION
   trident    21.04.0
   ```

   Trident가 없으면 다음과 유사한 출력이 표시됩니다.

   ```
   error: the server doesn't have a resource type "tridentversions"
   ```

   > Trident가 설치되지 않았거나 설치된 버전이 최신 버전이 아닌 경우 계속하기 전에 Trident의 최신 버전을 설치해야 합니다. 를 참조하십시오 "Trident 문서" 를 참조하십시오.

2. 스토리지 클래스가 지원되는 Trident 드라이버를 사용하고 있는지 확인합니다. 공급자 이름은 이어야 합니다

`csi.trident.netapp.io`. 다음 예를 참조하십시오.

```
kubectl get sc
NAME                    PROVISIONER                    RECLAIMPOLICY
VOLUMEBINDINGMODE   ALLOWVOLUMEEXPANSION   AGE
ontap-gold (default)    csi.trident.netapp.io          Delete
Immediate           true                   5d23h
thin                    kubernetes.io/vsphere-volume   Delete
Immediate           false                  6d
```

관리자 역할 **kubecononfig**를 생성합니다

단계를 수행하기 전에 시스템에 다음 사항이 있는지 확인하십시오.

- `kubectl` V1.19 이상이 설치되었습니다
- 활성 컨텍스트에 대한 클러스터 관리자 권한이 있는 활성 kubecononfig

단계

1. 다음과 같이 서비스 계정을 생성합니다.

   a. 라는 서비스 계정 파일을 생성합니다 `astracontrol-service-account.yaml`.

      필요에 따라 이름 및 네임스페이스를 조정합니다. 여기에서 변경한 경우 다음 단계에서 동일한 변경 사항을 적용해야 합니다.

```
<strong>astracontrol-service-account.yaml</strong>
```

+

```yaml
apiVersion: v1
kind: ServiceAccount
metadata:
  name: astracontrol-service-account
  namespace: default
```

   a. 서비스 계정 적용:

```
kubectl apply -f astracontrol-service-account.yaml
```

2. (선택 사항) 클러스터에서 권한이 있는 POD 생성을 허용하지 않거나 POD 컨테이너 내의 프로세스가 루트 사용자로 실행되도록 허용하지 않는 제한적인 POD 보안 정책을 사용하는 경우 Astra Control에서 POD를 생성 및 관리할 수 있도록 클러스터에 대한 사용자 지정 POD 보안 정책을 생성합니다. 자세한 내용은 을 참조하십시오 "사용자 지정 POD 보안 정책을 생성합니다".

3. 다음과 같이 클러스터 관리자 권한을 부여합니다.

   a. 을 생성합니다 `ClusterRoleBinding` 파일을 호출했습니다 `astracontrol-clusterrolebinding.yaml`.

      필요에 따라 서비스 계정을 생성할 때 수정된 모든 이름과 네임스페이스를 조정합니다.

```
<strong>astracontrol-clusterrolebinding.yaml</strong>
```

+

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: astracontrol-admin
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-admin
subjects:
- kind: ServiceAccount
  name: astracontrol-service-account
  namespace: default
```

   a. 클러스터 역할 바인딩을 적용합니다.

```
kubectl apply -f astracontrol-clusterrolebinding.yaml
```

4. 교체 서비스 계정 암호를 나열합니다 `<context>` 올바른 설치 상황:

```
kubectl get serviceaccount astracontrol-service-account --context
<context> --namespace default -o json
```

출력의 끝은 다음과 유사합니다.

```
"secrets": [
{ "name": "astracontrol-service-account-dockercfg-vhz87"},
{ "name": "astracontrol-service-account-token-r59kr"}
]
```

의 각 요소에 대한 인덱스입니다 `secrets` 어레이는 0으로 시작합니다. 위의 예에서 의 인덱스입니다 `astracontrol-service-account-dockercfg-vhz87` 는 0이고 의 인덱스입니다 `astracontrol-`

`service-account-token-r59kr` 1입니다. 출력에서 "token"이라는 단어가 포함된 서비스 계정 이름의 인덱스를 기록해 둡니다.

5. 다음과 같이 kubecononfig를 생성합니다.

   a. 을 생성합니다 `create-kubeconfig.sh` 파일. 대치 `TOKEN_INDEX` 다음 스크립트의 시작 부분에 올바른 값이 있습니다.

```
<strong>create-kubeconfig.sh</strong>
```

```
# Update these to match your environment.
# Replace TOKEN_INDEX with the correct value
# from the output in the previous step. If you
# didn't change anything else above, don't change
# anything else here.

SERVICE_ACCOUNT_NAME=astracontrol-service-account
NAMESPACE=default
NEW_CONTEXT=astracontrol
KUBECONFIG_FILE='kubeconfig-sa'

CONTEXT=$(kubectl config current-context)

SECRET_NAME=$(kubectl get serviceaccount ${SERVICE_ACCOUNT_NAME} \
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.secrets[TOKEN_INDEX].name}')
TOKEN_DATA=$(kubectl get secret ${SECRET_NAME} \
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.data.token}')

TOKEN=$(echo ${TOKEN_DATA} | base64 -d)

# Create dedicated kubeconfig
# Create a full copy
kubectl config view --raw > ${KUBECONFIG_FILE}.full.tmp

# Switch working context to correct context
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp config use-context
${CONTEXT}

# Minify
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp \
  config view --flatten --minify > ${KUBECONFIG_FILE}.tmp
```

```
# Rename context
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  rename-context ${CONTEXT} ${NEW_CONTEXT}

# Create token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-credentials ${CONTEXT}-${NAMESPACE}-token-user \
  --token ${TOKEN}

# Set context to use token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --user ${CONTEXT}-${NAMESPACE}-token
-user

# Set context to correct namespace
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --namespace ${NAMESPACE}

# Flatten/minify kubeconfig
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  view --flatten --minify > ${KUBECONFIG_FILE}

# Remove tmp
rm ${KUBECONFIG_FILE}.full.tmp
rm ${KUBECONFIG_FILE}.tmp
```

b. Kubernetes 클러스터에 적용할 명령을 소스 하십시오.

```
source create-kubeconfig.sh
```

6. (* 선택 사항 *) kubeconfig의 이름을 클러스터의 의미 있는 이름으로 바꿉니다. 클러스터 자격 증명을 보호합니다.

```
chmod 700 create-kubeconfig.sh
mv kubeconfig-sa.txt YOUR_CLUSTER_NAME_kubeconfig
```

다음 단계

이제 필수 구성 요소가 충족되었는지 확인했으므로 이제 수행할 준비가 되었습니다 "클러스터를 추가합니다".

자세한 내용을 확인하십시오

- "Trident 문서"
- "Astra Control API를 사용합니다"

사용자 지정 **TLS** 인증서를 추가합니다

기존의 자체 서명된 TLS 인증서를 제거하고 CA(인증 기관)에서 서명한 TLS 인증서로 바꿀 수 있습니다.

필요한 것

- Astra Control Center가 설치된 Kubernetes 클러스터
- 실행할 클러스터의 명령 셸에 대한 관리 액세스 `kubectl` 명령
- CA의 개인 키 및 인증서 파일

자체 서명된 인증서를 제거합니다

기존의 자체 서명된 TLS 인증서를 제거합니다.

1. SSH를 사용하여 관리 사용자로 Astra Control Center를 호스팅하는 Kubernetes 클러스터에 로그인합니다.
2. 다음 명령을 사용하여 현재 인증서와 연결된 TLS 암호를 찾아 바꿉니다 `<ACC-deployment-namespace>` Astra Control Center 배포 네임스페이스 사용:

```
kubectl get certificate -n <ACC-deployment-namespace>
```

3. 다음 명령을 사용하여 현재 설치된 암호 및 인증서를 삭제합니다.

```
kubectl delete cert cert-manager-certificates -n <ACC-deployment-
namespace>
kubectl delete secret secure-testing-cert -n <ACC-deployment-namespace>
```

새 인증서를 추가합니다

CA에서 서명한 새 TLS 인증서를 추가합니다.

1. 다음 명령을 사용하여 CA의 개인 키 및 인증서 파일로 새 TLS 암호를 만들고 대괄호 <>의 인수를 적절한 정보로 바꿉니다.

```
kubectl create secret tls <secret-name> --key <private-key-filename>
--cert <certificate-filename> -n <ACC-deployment-namespace>
```

2. 다음 명령 및 예제를 사용하여 클러스터 CRD(Custom Resource Definition) 파일을 편집하고 를 변경합니다 `spec.selfSigned` 값을 로 설정합니다 `spec.ca.secretName` 앞에서 만든 TLS 암호를 확인하려면 다음을 수행하십시오.

```
kubectl edit clusterissuers.cert-manager.io/cert-manager-certificates -n
<ACC-deployment-namespace>
....

#spec:
#  selfSigned: {}

spec:
  ca:
    secretName: <secret-name>
```

3. 다음 명령 및 예제 출력을 사용하여 변경 사항이 올바른지, 클러스터가 인증서를 교체할 준비가 되었는지 확인합니다 `<ACC-deployment-namespace>` Astra Control Center 배포 네임스페이스 사용:

```
kubectl describe clusterissuers.cert-manager.io/cert-manager-
certificates -n <ACC-deployment-namespace>
....

Status:
  Conditions:
    Last Transition Time:  2021-07-01T23:50:27Z
    Message:               Signing CA verified
    Reason:                KeyPairVerified
    Status:                True
    Type:                  Ready
Events:                    <none>
```

4. 를 생성합니다 `certificate.yaml` 다음 예제를 사용하는 파일 대괄호 <>의 개체 틀 값을 적절한 정보로 바꿉니다.

```yaml
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: <certificate-name>
  namespace: <ACC-deployment-namespace>
spec:
  secretName: <certificate-secret-name>
  duration: 2160h # 90d
  renewBefore: 360h # 15d
  dnsNames:
  - <astra.dnsname.example.com> #Replace with the correct Astra Control
Center DNS address
  issuerRef:
    kind: ClusterIssuer
    name: cert-manager-certificates
```

5. 다음 명령을 사용하여 인증서를 생성합니다.

```
kubectl apply -f certificate.yaml
```

6. 다음 명령 및 예제 출력을 사용하여 인증서가 올바르게 만들어졌는지, 그리고 생성 중에 지정한 인수(예: 이름, 기간, 갱신 기한 및 DNS 이름)를 사용하여 확인합니다.

```
kubectl describe certificate -n <ACC-deployment-namespace>
....

Spec:
  Dns Names:
    astra.example.com
  Duration:  125h0m0s
  Issuer Ref:
    Kind:        ClusterIssuer
    Name:        cert-manager-certificates
  Renew Before:  61h0m0s
  Secret Name:   <certificate-secret-name>
Status:
  Conditions:
    Last Transition Time:  2021-07-02T00:45:41Z
    Message:               Certificate is up to date and has not expired
    Reason:                Ready
    Status:                True
    Type:                  Ready
  Not After:               2021-07-07T05:45:41Z
  Not Before:              2021-07-02T00:45:41Z
  Renewal Time:            2021-07-04T16:45:41Z
  Revision:                1
Events:                    <none>
```

7. 다음 명령 및 예제를 사용하여 새 인증서 암호를 가리키도록 수신 CRD TLS 옵션을 편집합니다. 대괄호 <>의 개체 틀 값을 적절한 정보로 바꿉니다.

```
kubectl edit ingressroutes.traefik.containo.us -n <ACC-deployment-
namespace>
....

# tls:
#    options:
#      name: default
#    secretName: secure-testing-cert
#    store:
#      name: default

 tls:
    options:
      name: default
    secretName: <certificate-secret-name>
    store:
      name: default
```

8. 웹 브라우저를 사용하여 Astra Control Center의 배포 IP 주소로 이동합니다.
9. 인증서 세부 정보가 설치한 인증서의 세부 정보와 일치하는지 확인합니다.
10. 인증서를 내보내고 결과를 웹 브라우저의 인증서 관리자로 가져옵니다.

사용자 지정 **POD** 보안 정책을 생성합니다

Astra Control은 관리하는 클러스터에서 Kubernetes Pod를 생성 및 관리해야 합니다. 클러스터에서 권한이 있는 POD 생성을 허용하지 않거나 POD 컨테이너 내의 프로세스가 루트 사용자로 실행되도록 허용하는 제한적인 POD 보안 정책을 사용하는 경우, Astra Control에서 이러한 POD를 생성 및 관리할 수 있도록 덜 제한적인 POD 보안 정책을 만들어야 합니다.

단계

1. 기본값보다 덜 제한적인 클러스터에 대한 POD 보안 정책을 생성하여 파일에 저장합니다. 예를 들면 다음과 같습니다.

```yaml
apiVersion: policy/v1beta1
kind: PodSecurityPolicy
metadata:
  name: astracontrol
  annotations:
    seccomp.security.alpha.kubernetes.io/allowedProfileNames: '*'
spec:
  privileged: true
  allowPrivilegeEscalation: true
  allowedCapabilities:
  - '*'
  volumes:
  - '*'
  hostNetwork: true
  hostPorts:
  - min: 0
    max: 65535
  hostIPC: true
  hostPID: true
  runAsUser:
    rule: 'RunAsAny'
  seLinux:
    rule: 'RunAsAny'
  supplementalGroups:
    rule: 'RunAsAny'
  fsGroup:
    rule: 'RunAsAny'
```

2. POD 보안 정책에 대한 새 역할을 생성합니다.

```bash
kubectl-admin create role psp:astracontrol \
    --verb=use \
    --resource=podsecuritypolicy \
    --resource-name=astracontrol
```

3. 새 역할을 서비스 계정에 바인딩합니다.

```bash
kubectl-admin create rolebinding default:psp:astracontrol \
    --role=psp:astracontrol \
    --serviceaccount=astracontrol-service-account:default
```

Astra Control Center에 대한 질문과 대답

이 FAQ는 질문에 대한 간단한 답변을 찾는 경우에 도움이 될 수 있습니다.

개요

다음 섹션에서는 Astra Control Center를 사용할 때 나타날 수 있는 몇 가지 추가 질문에 대한 답변을 제공합니다. 자세한 내용은 astra.feedback@netapp.com 으로 문의하십시오

Astra Control Center에 액세스할 수 있습니다

- Astra Control URL은 무엇입니까? *

Astra Control Center는 로컬 인증과 각 환경에 고유한 URL을 사용합니다.

URL의 경우 브라우저에서 Astra_control_center_min YAML 사용자 정의 리소스 정의(CRD) 파일(Astra Control Center 설치 시)의 spec.astraAddress 필드에 설정한 FQDN(정규화된 도메인 이름)을 입력합니다. 이메일은 Astra_control_center_min YAML CRD의 spec.email 필드에 설정한 값입니다.

라이센싱

- 평가판 라이센스를 사용하고 있습니다. 전체 라이센스로 변경하는 방법은 무엇입니까? *

NetApp 라이센스 파일(NLF)을 받아 전체 라이센스로 쉽게 변경할 수 있습니다.

- 단계 *
- 왼쪽 탐색 창에서 * 계정 * > * 라이센스 * 를 선택합니다.
- 라이선스 추가 * 를 선택합니다.
- 다운로드한 라이센스 파일을 찾아 * 추가 * 를 선택합니다.
- 평가판 라이센스를 사용하고 있습니다. 앱을 관리할 수 있습니까? *

예. 평가판 라이센스를 사용하여 관리 앱 기능을 테스트할 수 있습니다.

Kubernetes 클러스터를 등록하는 중입니다

- Astra Control에 추가한 후 Kubernetes 클러스터에 작업자 노드를 추가해야 합니다. 어떻게 해야 합니까? *

새 작업자 노드를 기존 풀에 추가할 수 있습니다. 이러한 정보는 Astra Control에서 자동으로 발견됩니다. Astra Control에서 새 노드가 보이지 않으면 새 작업자 노드가 지원되는 이미지 유형을 실행하고 있는지 확인합니다. 을 사용하여 새 작업자 노드의 상태를 확인할 수도 있습니다 `kubectl get nodes` 명령.

- 클러스터를 올바르게 관리하려면 어떻게 해야 합니까? *
  1. "Astra Control에서 애플리케이션을 관리합니다".
  2. "Astra Control에서 클러스터 관리를 해제합니다".
- Astra Control에서 Kubernetes 클러스터를 제거한 후 애플리케이션과 데이터는 어떻게 됩니까? *

Astra Control에서 클러스터를 제거해도 클러스터의 구성(애플리케이션 및 영구 스토리지)은 변경되지 않습니다. Astra

Control 스냅샷 또는 해당 클러스터의 애플리케이션 백업을 복구할 수 없습니다. Astra Control에서 생성한 영구 스토리지 백업은 Astra Control 내에 남아 있지만 복구할 수 없습니다.

> 다른 방법을 통해 클러스터를 삭제하기 전에 항상 Astra Control에서 클러스터를 제거하십시오. Astra Control에서 관리하는 다른 도구를 사용하여 클러스터를 삭제하면 Astra Control 계정에 문제가 발생할 수 있습니다.

- 관리를 해제하면 NetApp Trident가 클러스터에서 자동으로 제거됩니까? * Astra Control Center에서 클러스터를 관리할 때 Trident가 클러스터에서 자동으로 제거되지 않습니다. Trident를 제거하려면 가 필요합니다 "Trident 문서의 다음 단계를 따릅니다".

응용 프로그램 관리

- Astra Control이 응용 프로그램을 배포할 수 있습니까? *

Astra Control은 애플리케이션을 배포하지 않습니다. 응용 프로그램은 Astra Control 외부에서 배포해야 합니다.

- Astra Control에서 관리를 중지한 후 응용 프로그램은 어떻게 됩니까? *

기존 백업 또는 스냅샷이 삭제됩니다. 애플리케이션과 데이터는 사용 가능한 상태로 유지됩니다. 관리되지 않는 응용 프로그램 또는 해당 응용 프로그램에 속한 백업 또는 스냅숏에는 데이터 관리 작업을 사용할 수 없습니다.

- Astra Control이 NetApp이 아닌 스토리지에 있는 애플리케이션을 관리할 수 있습니까? *

아니요 Astra Control은 NetApp이 아닌 스토리지를 사용하는 애플리케이션을 검색할 수 있지만, NetApp이 아닌 스토리지를 사용하는 애플리케이션은 관리할 수 없습니다.

"Astra Control 자체를 관리해야 하나요?" "아닙니다. Astra Control 자체는 "시스템 앱"이기 때문에 관리하지 말아야 합니다.

- 비정상적인 포드가 앱 관리에 영향을 미치나요? * 관리 애플리케이션에 상태가 불량한 포드가 있는 경우, Astra Control은 새 백업 및 클론을 생성할 수 없습니다.

데이터 관리 작업

- 내 계정에 생성하지 않은 스냅샷이 있습니다. 어디에서 왔습니까? *

일부 상황에서는 Astra Control이 백업, 클론 또는 복원 프로세스의 일부로 스냅샷을 자동으로 생성합니다.

- My Application은 여러 PVS를 사용합니다. Astra Control이 이러한 모든 PVC의 스냅샷 및 백업을 수행할까요? *

예. Astra Control의 애플리케이션에 대한 스냅샷 작업에는 애플리케이션의 PVC에 바인딩된 모든 PVS의 스냅샷이 포함됩니다.

- Astra Control에서 생성한 스냅샷을 다른 인터페이스 또는 객체 스토리지를 통해 직접 관리할 수 있습니까? *

아니요 Astra Control에서 생성한 스냅샷 및 백업은 Astra Control에서만 관리할 수 있습니다.

Astra를 사용하십시오

앱 관리를 시작합니다

먼저 해 "Astra Control 관리에 클러스터를 추가합니다", 클러스터(Astra Control 외부)에 앱을 설치한 다음 Astra Control의 애플리케이션 페이지로 이동하여 앱과 리소스 관리를 시작할 수 있습니다.

자세한 내용은 을 참조하십시오 "설명합니다".

지원되는 앱 설치 방법

Astra Control은 다음과 같은 응용 프로그램 설치 방법을 지원합니다.

- * 매니페스트 파일 *: Astra Control은 kubctl을 사용하여 매니페스트 파일에서 설치된 앱을 지원합니다. 예를 들면 다음과 같습니다.

  ```
  kubectl apply -f myapp.yaml
  ```

- * Helm 3 *: Helm을 사용하여 앱을 설치하는 경우 Astra Control에 Helm 버전 3이 필요합니다. Helm 3(또는 Helm 2에서 Helm 3으로 업그레이드)과 함께 설치된 앱의 관리 및 클론 생성이 완벽하게 지원됩니다. Helm 2가 설치된 앱 관리는 지원되지 않습니다.
- * 운용자 구축 앱 *: Astra Control은 네임스페이스 범위 연산자로 설치된 앱을 지원합니다. 일반적으로 "pass-by-reference" 아키텍처가 아니라 "pass-by-value"로 설계되었습니다. 운영자와 설치하는 앱은 동일한 네임스페이스를 사용해야 합니다. 운영자가 배포 .YAML 파일을 수정해야 할 수도 있습니다.

  다음은 이러한 패턴을 따르는 일부 운영자 앱에 대한 설명입니다.

  - "아파치 K8ssandra"

    > K8ssandra 의 경우 현재 위치 복원 작업이 지원됩니다. 새 네임스페이스 또는 클러스터에 대한 복원 작업을 수행하려면 응용 프로그램의 원래 인스턴스를 중단해야 합니다. 이는 이월된 피어 그룹 정보가 인스턴스 간 통신으로 이어지지 않도록 하기 위한 것입니다. 앱 복제는 지원되지 않습니다.

  - "젠킨스 CI"
  - "Percona XtraDB 클러스터"

Astra Control은 "pass-by-reference" 아키텍처(예: CockroachDB 운영자)로 설계된 운영자를 복제하지 못할 수 있습니다. 이러한 유형의 클론 복제 작업 중에 클론 복제 운영자는 클론 복제 프로세스의 일부로 고유한 새로운 암호가 있음에도 불구하고 소스 운영자의 Kubernetes 암호를 참조하려고 합니다. Astra Control이 소스 운영자의 Kubernetes 암호를 모르기 때문에 클론 작업이 실패할 수 있습니다.

클러스터에 앱을 설치합니다

먼저 해 "클러스터가 추가되었습니다" Astra Control은 클러스터에서 앱을 설치하거나 기존 앱을 관리할 수 있습니다. 단일 네임스페이스로 범위가 지정된 모든 앱을 관리할 수 있습니다.

앱 관리

Astra Control이 클러스터에서 네임스페이스를 검색한 후 관리할 애플리케이션을 정의할 수 있습니다. 선택할 수 있습니다 "전체 네임스페이스를 단일 애플리케이션으로 관리하거나 네임스페이스에서 개별적으로 하나 이상의 앱을 관리합니다". 데이터 보호 작업에 필요한 세분화 수준으로 세분화됩니다.

Astra Control을 사용하면 계층 구조의 수준(네임스페이스 및 해당 네임스페이스의 앱)을 모두 개별적으로 관리할 수 있지만 가장 좋은 방법은 하나 또는 다른 수준을 선택하는 것입니다. 작업이 네임스페이스 및 앱 수준에서 동시에 발생하면 Astra Control에서 수행하는 작업이 실패할 수 있습니다.

> 예를 들어, "Maria"에 대해 주간 백업 주기를 갖는 백업 정책을 설정할 수 있지만 "MariaDB"(동일한 네임스페이스)를 더 자주 백업해야 할 수 있습니다. 이러한 요구사항에 따라 단일 네임스페이스 앱이 아니라 앱을 별도로 관리해야 합니다.

필요한 것

- Astra Control에 Kubernetes 클러스터가 추가되었습니다.
- 클러스터에 설치된 애플리케이션 하나 이상 지원되는 앱 설치 방법에 대해 자세히 알아보십시오.
- 하나 이상의 활성 포드.
- Astra Control에 추가한 Kubernetes 클러스터에 지정된 네임스페이스입니다.
- (선택 사항) 모든 Kubernetes 레이블 "지원되는 Kubernetes 리소스".

> 레이블은 식별을 위해 Kubernetes 객체에 할당할 수 있는 키/값 쌍입니다. 레이블을 사용하면 Kubernetes 오브젝트를 더 쉽게 정렬, 구성 및 찾을 수 있습니다. Kubernetes 레이블에 대해 자세히 알아보려면 "Kubernetes 공식 문서를 참조하십시오".

시작하기 전에, 또한 이해해야 합니다 "표준 및 시스템 네임스페이스 관리".

Astra Control API를 사용하여 앱을 관리하는 방법에 대한 지침은 를 참조하십시오 "Astra 자동화 및 API 정보".

애플리케이션 관리 옵션

- 앱으로 관리할 리소스를 정의합니다
- 앱으로 관리할 네임스페이스를 정의합니다

추가 앱 관리 옵션

- 앱 관리 취소

앱으로 관리할 리소스를 정의합니다

를 지정할 수 있습니다 "앱을 구성하는 Kubernetes 리소스" Astra Control을 통해 관리하고자 하는 것입니다. 앱을 정의하면 Kubernetes 클러스터의 요소를 단일 애플리케이션으로 그룹화할 수 있습니다. 이 Kubernetes 리소스 모음은 네임스페이스 및 레이블 선택기 기준에 따라 구성됩니다.

앱을 정의하면 클론, 스냅샷, 백업을 비롯한 Astra Control 작업에 포함할 항목을 보다 세부적으로 제어할 수 있습니다.

> 앱을 정의할 때 보호 정책이 있는 여러 앱에 Kubernetes 리소스를 포함하지 않아야 합니다. Kubernetes 리소스의 보호 정책이 중복되어 데이터 충돌이 발생할 수 있습니다. 모범 사례에 대해 자세히 알아보십시오.

단계

1. 응용 프로그램 페이지에서 * 정의 * 를 선택합니다.
2. 응용 프로그램 정의 * 창에서 응용 프로그램 이름을 입력합니다.
3. 응용 프로그램이 실행되는 클러스터를 * 클러스터 * 드롭다운 목록에서 선택합니다.
4. Namespace* 드롭다운 목록에서 응용 프로그램의 네임스페이스를 선택합니다.

> 앱은 단일 클러스터에서 지정된 네임스페이스 내에서만 정의할 수 있습니다. Astra Control은 앱이 여러 네임스페이스 또는 클러스터를 확장하는 기능을 지원하지 않습니다.

5. 앱 및 네임스페이스의 레이블을 입력합니다. 단일 레이블 또는 레이블 선택 조건(쿼리)을 지정할 수 있습니다.

> Kubernetes 레이블에 대해 자세히 알아보려면 "Kubernetes 공식 문서를 참조하십시오".

6. 정의 * 를 선택한 후 필요에 따라 다른 앱에 대해 프로세스를 반복합니다.

앱 정의를 마치면 응용 프로그램 페이지의 앱 목록에 앱이 나타납니다. 이제 클론을 생성하고 백업과 스냅샷을 생성할 수 있습니다.

> 방금 추가한 앱에는 Protected(보호) 열 아래에 백업이 없고 아직 백업이 예약되지 않았음을 나타내는 경고 아이콘이 있을 수 있습니다.

> 특정 앱의 세부 정보를 보려면 앱 이름을 선택합니다.

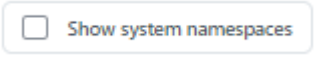
앱으로 관리할 네임스페이스를 정의합니다

네임스페이스의 리소스를 애플리케이션으로 정의하여 Astra Control 관리에 네임스페이스의 모든 Kubernetes 리소스를 추가할 수 있습니다. 이 방법은 특정 네임스페이스의 모든 리소스를 비슷한 방식으로 일정한 간격으로 관리하고 보호하려는 경우 앱을 개별적으로 정의하는 것이 좋습니다.

단계

1. 클러스터 페이지에서 클러스터를 선택합니다.
2. Namespaces* 탭을 선택합니다.
3. 관리하려는 앱 리소스가 포함된 네임스페이스의 작업 메뉴를 선택하고 * 응용 프로그램으로 정의 * 를 선택합니다.

> 여러 네임스페이스를 관리하려면 네임스페이스를 선택하고 왼쪽 위 모서리에 있는 * Actions * 버튼을 선택하고 * manage * 를 선택합니다.

> 기본적으로 앱 관리에 사용되지 않는 시스템 네임스페이스를 표시하려면 * Show system namespaces * 확인란을 선택합니다. 

"자세히 보기".

프로세스가 완료되면 네임스페이스와 연결된 응용 프로그램이 에 나타납니다 `Associated applications` 열.

앱 관리 취소

더 이상 앱을 백업, 스냅샷 또는 클론 복제하지 않으려는 경우 관리를 중지할 수 있습니다.

> 앱 관리를 해제하면 이전에 생성된 모든 백업 또는 스냅샷이 손실됩니다.

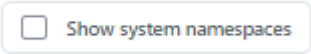
단계

1. 왼쪽 탐색 모음에서 * 응용 프로그램 * 을 선택합니다.
2. 앱을 선택합니다.
3. Actions * 열의 메뉴에서 * Unmanage * 를 선택합니다.
4. 정보를 검토합니다.
5. "unmanage"를 입력하여 확인합니다.
6. 예, 응용 프로그램 관리 취소 * 를 선택합니다.

시스템 네임스페이스는 어떻습니까?

Astra Control은 Kubernetes 클러스터에서 시스템 네임스페이스를 검색합니다. 기본적으로 이러한 시스템 네임스페이스는 표시되지 않습니다. 시스템 앱 리소스를 백업해야 하는 경우는 드뭅니다.

선택한 클러스터의 Namespaces 탭에서 * Show system namespaces * 확인란을 선택하여 시스템 네임스페이스를 표시할 수 있습니다.



> Astra Control 자체는 표준 앱이 아니며 "시스템 앱"입니다. Astra Control 자체를 관리하려고 해서는 안 됩니다. 관리 시 Astra Control 자체는 기본적으로 표시되지 않습니다.

예: 다른 릴리즈에 대한 별도의 보호 정책

이 예제에서 DevOps 팀은 "카나리아" 릴리스 배포를 관리합니다. 팀의 클러스터에는 Nginx를 실행하는 3개의 포드가 있습니다. 포드 중 2개는 안정적인 릴리스 전용입니다. 세 번째 포드는 카나리 해제 시 사용합니다.

DevOps 팀의 Kubernetes 관리자가 레이블을 추가합니다 `deployment=stable` 안정적인 분리 포드로. 팀에서 라벨을 추가합니다 `deployment=canary` 캔리 분리 포드로.

이 팀의 안정적인 릴리즈에는 시간별 스냅샷 및 일일 백업에 대한 요구 사항이 포함됩니다. 카나리아 릴리스는 수명이 짧기 때문에 레이블이 지정된 모든 것에 대해 공격적이고 단기적인 보호 정책을 만들고자 합니다 `deployment=canary`.

데이터 충돌을 방지하기 위해 관리자는 "Canary" 릴리스용 앱과 "Stable" 릴리즈용 앱을 두 개 만듭니다. 이렇게 하면 두 Kubernetes 객체 그룹에 대해 백업, 스냅샷 및 클론 작업이 분리됩니다.

자세한 내용을 확인하십시오

- "Astra Control API를 사용합니다"

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 UI 또는 를 사용할 수 있습니다 "Astra Control API" 앱을 보호합니다.

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 클러스터에서 앱을 호스팅하기 위한 프로젝트를 만들면 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
- 스냅샷 및 백업을 봅니다
- 스냅샷을 삭제합니다
- 백업을 취소합니다
- 백업을 삭제합니다

보호 정책을 구성합니다

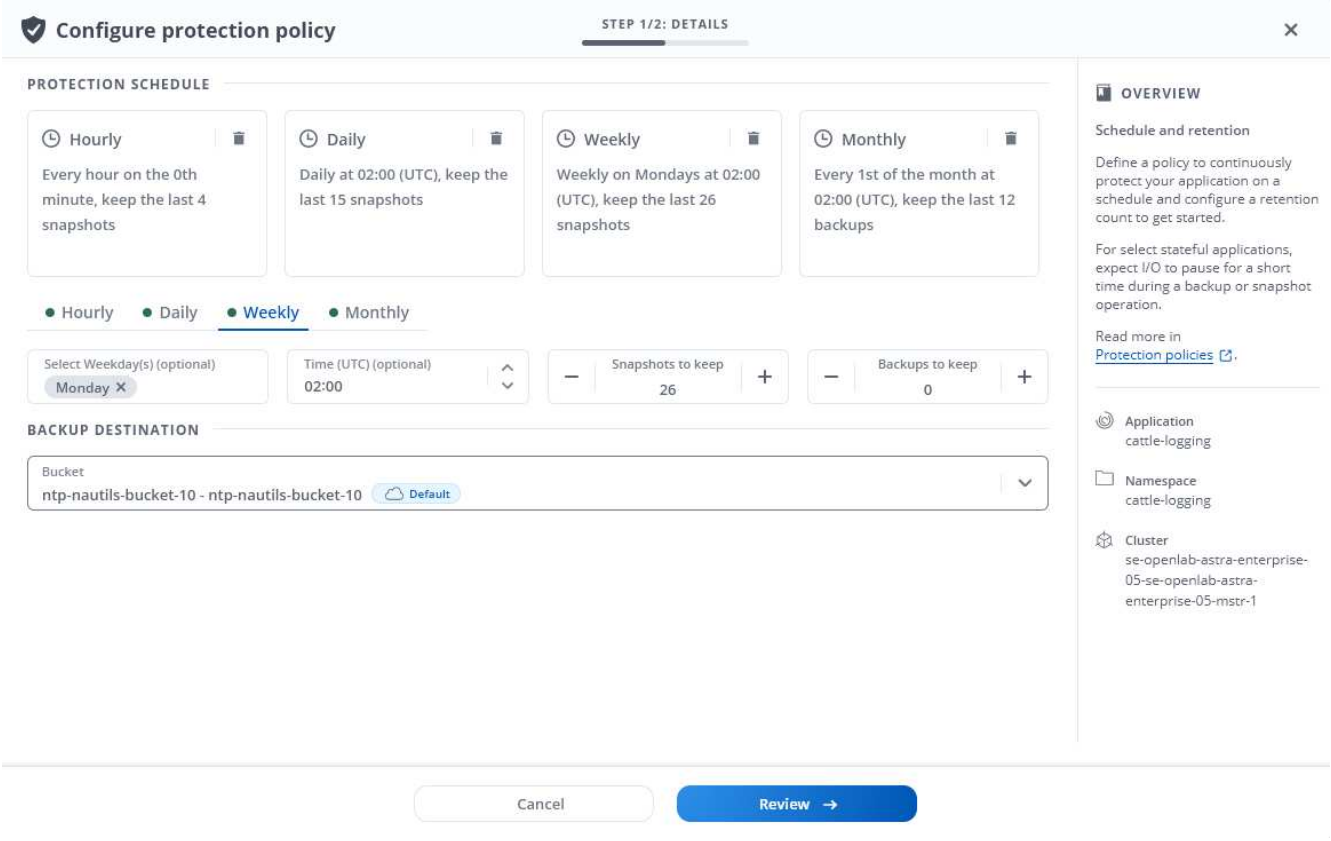
보호 정책은 정의된 일정에 따라 스냅샷, 백업 또는 둘 다를 생성하여 앱을 보호합니다. 시간별, 일별, 주별 및 월별 스냅샷과 백업을 생성하도록 선택할 수 있으며, 보존할 복제본 수를 지정할 수 있습니다. 예를 들어 보호 정책은 주별 백업과 일별 스냅샷을 생성하고 백업 및 스냅샷을 한 달 동안 보존할 수 있습니다. 스냅샷 및 백업을 생성하는 빈도와 보관 기간은 조직의 요구 사항에 따라 다릅니다.

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.

   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 Control Center는 사용자가 정의한 스케줄 및 보존 정책을 사용하여 스냅샷 및 백업을 생성하고 유지함으로써 데이터 보호 정책을 구현합니다.

스냅샷을 생성합니다

언제든지 주문형 스냅샷을 생성할 수 있습니다.

단계

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

결과

스냅샷 프로세스가 시작됩니다. 데이터 보호 * > * 스냅샷 * 페이지의 * 작업 * 열에서 * 사용 가능 * 상태가 되면 스냅샷이 성공적으로 생성됩니다.

백업을 생성합니다

언제든지 앱을 백업할 수도 있습니다.

> 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.

단계

1. 응용 프로그램 * 을 선택합니다.
2. 원하는 앱의 * Actions * 열에 있는 옵션 메뉴에서 * Backup * 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 선택하여 백업 대상을 선택합니다.
6. Review * 를 선택합니다.
7. 백업 요약을 검토하고 * Backup * 을 선택합니다.

결과

Astra Control Center는 앱 백업을 생성합니다.

> 네트워크에 정전이 발생했거나 비정상적으로 느린 경우 백업 작업이 시간 초과될 수 있습니다. 이로 인해 백업이 실패합니다.

> 실행 중인 백업을 중지할 방법은 없습니다. 백업을 삭제해야 하는 경우 백업이 완료될 때까지 기다린 다음 의 지침을 따르십시오 백업을 삭제합니다. 실패한 백업을 삭제하려면 "Astra Control API를 사용합니다".

> 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.

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 스냅샷 복사본은 삭제할 수 없습니다.

단계

1. 응용 프로그램 * 을 선택한 다음 앱 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 Control Center가 스냅샷을 삭제합니다.

백업을 취소합니다

진행 중인 백업을 취소할 수 있습니다.

> 백업을 취소하려면 백업이 실행 중 상태여야 합니다. 보류 중인 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. 삭제를 확인하려면 "취소"라는 단어를 입력하고 * 예, 백업 취소 * 를 선택합니다.

백업을 삭제합니다

더 이상 필요하지 않은 예약된 백업 또는 필요 시 백업을 삭제합니다.

> 실행 중인 백업을 중지할 방법은 없습니다. 백업을 삭제해야 하는 경우 백업이 완료될 때까지 기다린 후 다음 지침을 따르십시오. 실패한 백업을 삭제하려면 "Astra Control API를 사용합니다".

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 Control Center가 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 API" 앱을 복원합니다.

이 작업에 대해

- 응용 프로그램을 복원하기 전에 응용 프로그램의 스냅샷을 생성하거나 백업하는 것이 좋습니다. 이렇게 하면 복구에 실패한 경우 스냅샷 또는 백업에서 클론을 생성할 수 있습니다.
- 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.
- 다른 클러스터로 복원하는 경우 클러스터에서 동일한 영구 볼륨 액세스 모드(예: ReadWriteMany)를 사용하고 있는지 확인합니다. 대상 영구 볼륨 액세스 모드가 다르면 복원 작업이 실패합니다.
- 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 작업을 통해 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.
- OpenShift 클러스터에서 앱을 호스팅하기 위한 프로젝트를 만들면 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 선택한 다음 앱 이름을 선택합니다.
2. 데이터 보호 * 를 선택합니다.
3. 스냅샷에서 복구하려면 * 스냅샷 * 아이콘을 선택한 상태로 유지합니다. 그렇지 않으면 * Backups * 아이콘을 선택하여 백업에서 복원합니다.
4. 복원하려는 스냅샷 또는 백업의 * 작업 * 열에 있는 옵션 메뉴에서 * 응용 프로그램 복원 * 을 선택합니다.
5. * Restore details *: 복원된 앱에 대한 세부 정보를 지정합니다. 기본적으로 현재 클러스터와 네임스페이스가 표시됩니다. 앱을 원래 상태로 복원하려면 이 값을 그대로 두십시오. 이렇게 하면 앱이 이전 버전으로 되돌아갑니다. 다른 클러스터 또는 네임스페이스로 복원하려는 경우 이 값을 변경합니다.
   - 앱의 이름과 네임스페이스를 입력합니다.
   - 앱의 대상 클러스터를 선택합니다.
   - Review * 를 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.

6. * 복원 요약 *: 복원 작업에 대한 세부 정보를 검토하고 "복원"을 입력한 다음 * 복원 * 을 선택합니다.

결과

Astra Control Center는 사용자가 제공한 정보를 기반으로 앱을 복원합니다. 앱을 제자리에 복원한 경우 기존 영구

볼륨의 콘텐츠가 복원된 앱의 영구 볼륨 내용으로 바뀝니다.

> 데이터 보호 작업(클론, 백업, 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.

SnapMirror 기술을 사용하여 원격 시스템에 애플리케이션을 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 클러스터 간에 데이터 및 애플리케이션 변경사항을 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 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 클러스터 또는 사이트에서 실행 중인 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

를 참조하십시오 "복제 사전 요구 사항" 시작하기 전에.

복제 관계를 설정합니다

복제 관계를 설정하려면 복제 정책을 구성하는 다음 작업이 필요합니다.

- Astra Control에서 애플리케이션 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 촬영할 시간 설정

단계

1. Astra Control 왼쪽 탐색 모음에서 * 응용 프로그램 * 을 선택합니다.
2. 애플리케이션 페이지에서 * 데이터 보호 * > * 복제 * 탭을 선택합니다.
3. 데이터 보호 > 복제 탭에서 * 복제 정책 구성 * 을 선택합니다. 또는 애플리케이션 보호 상자에서 작업 옵션을 선택하고 * 복제 정책 구성 * 을 선택합니다.
4. 다음 정보를 입력하거나 선택합니다.
   - 타겟 클러스터
   - * 대상 스토리지 클래스 *: 대상 ONTAP 클러스터에서 쌍을 이루는 SVM을 사용하는 스토리지 클래스를 선택하거나 입력합니다.
   - * 복제 유형 *: "비동기"는 현재 사용 가능한 유일한 복제 유형입니다.
   - * 대상 네임스페이스 *: 대상 클러스터에 대한 새 또는 기존 대상 네임스페이스를 입력합니다.

     ⓘ 선택한 네임스페이스의 충돌하는 모든 리소스를 덮어씁니다.

   - * 복제 빈도 *: Astra Control이 스냅샷을 생성하여 대상에 복제할 빈도를 설정합니다.
   - * 오프셋 *: Astra Control에서 스냅샷을 생성할 시간(분)을 설정합니다. 다른 예약된 작업과 일치하지 않도록 오프셋을 사용할 수 있습니다. 예를 들어 10:02부터 5분마다 스냅샷을 만들려는 경우 오프셋 분으로 "02"를 입력합니다. 결과는 10:02, 10:07, 10:12 등이 될 것입니다
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 "replication-schedule-<string>" 형식을 사용합니다. 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 Snapshot을 만듭니다.
- 초기 스냅샷을 사용하여 영구 볼륨의 SnapMirror 관계를 설정합니다.

데이터 보호 페이지에는 복제 관계 상태 및 상태가 표시됩니다. <상태>|<관계 수명 주기 상태>

예: Normal | 설정합니다

아래에서 복제 상태 및 상태에 대해 자세히 알아보십시오.

대상 클러스터에서 복제된 앱을 온라인 상태로 전환(페일오버)

Astra Control을 사용하면 복제된 애플리케이션을 대상 클러스터로 "페일오버"할 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. 애플리케이션 페이지에서 * 데이터 보호 * > * 복제 * 탭을 선택합니다.
3. 데이터 보호 > 복제 탭의 작업 메뉴에서 * 페일오버 * 를 선택합니다.
4. 페일오버 페이지에서 정보를 검토하고 * 페일오버 * 를 선택합니다.

결과

페일오버 절차로 인해 다음 작업이 수행됩니다.

- 대상 클러스터에서 최신 복제 스냅샷을 기반으로 앱이 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 장애 조치 시 소스 앱에 있는 일정에 따라 대상 앱에 복사됩니다.
- 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. 애플리케이션 페이지에서 * 데이터 보호 * > * 복제 * 탭을 선택합니다.
3. 데이터 보호 > 복제 탭의 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 클러스터로 계속 복제하면서 애플리케이션을 대상 클러스터로 이동하기 위한 계획된 작업입니다. Astra Control은 소스 클러스터에서 애플리케이션을 중지하고 대상 클러스터에 앱을 페일오버하기 전에 데이터를 대상에 복제합니다.

이 경우 소스와 대상을 스와핑합니다. 원래 소스 클러스터가 새 대상 클러스터가 되고 원래 타겟 클러스터가 새 소스 클러스터가 됩니다.

단계

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

결과

역방향 복제의 결과로 다음 작업이 수행됩니다.

- 원본 소스 앱의 Kubernetes 리소스 에 대한 스냅샷이 촬영됩니다.
- 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 Snapshot에서 복원됩니다.
- 복제는 반대 방향으로 다시 설정됩니다.

애플리케이션을 원래 소스 클러스터로 페일백합니다

Astra Control을 사용하면 다음과 같은 일련의 작업을 통해 "장애 조치" 작업 후에 "장애 복구"를 달성할 수 있습니다. 이 워크플로우에서 원래 복제 방향을 복구하기 위해 Astra Control은 복제 방향을 바꾸기 전에 애플리케이션 변경 사항을 원래 소스 클러스터로 복제(재동기화)합니다.

이 프로세스는 대상에 대한 장애 조치를 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. 애플리케이션 페이지에서 * 데이터 보호 * > * 복제 * 탭을 선택합니다.
3. 데이터 보호 > 복제 탭의 작업 메뉴에서 * 재동기화 * 를 선택합니다.
4. 장애 복구 작업의 경우 페일오버된 앱을 재동기화 작업의 소스로 선택합니다(기록된 모든 데이터 장애 조치 유지).
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. 애플리케이션 페이지에서 * 데이터 보호 * > * 복제 * 탭을 선택합니다.
3. 데이터 보호 > 복제 탭의 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(성공한 스냅샷은 복제되고 페일오버는 가능) 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 앱의 스냅샷을 생성하고, 앱에서 새로운 소스 PVC를 식별합니다. 이 경우 Astra Control은 복제에 포함할 리소스를 생성합니다.
- * 페일오버 *: Astra Control은 SnapMirror 관계를 중단시키고 마지막으로 성공한 복제 애플리케이션 Snapshot에서 앱의 Kubernetes 리소스를 복원합니다.
- * 페일오버됨 *: Astra Control은 소스 클러스터에서 복제를 중지하고, 대상에서 최근(성공한) 복제 앱 Snapshot을 사용하고, 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 생성합니다. Astra Control Center에서 앱을 클론하면 애플리케이션 구성 및 영구 스토리지의 클론이 생성됩니다.

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 UI 또는 를 사용할 수 있습니다 "Astra Control API" 앱을 클론 복제 및 마이그레이션합니다.

필요한 것

앱을 다른 클러스터로 클론 복제하려면 기본 버킷이 필요합니다. 첫 번째 버킷을 추가하면 기본 버킷을 사용할 수

있습니다.

이 작업에 대해

- StorageClass가 명시적으로 설정된 앱을 배포하고 앱을 복제해야 하는 경우 타겟 클러스터에 원래 지정된 StorageClass가 있어야 합니다. 명시적으로 StorageClass를 동일한 StorageClass가 없는 클러스터로 설정한 애플리케이션을 클론 복제하면 실패합니다.
- Jenkins CI의 운영자 배포 인스턴스를 복제하는 경우 영구 데이터를 수동으로 복원해야 합니다. 이는 앱 배포 모델의 제한 사항입니다.
- 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.
- 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.
- 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 작업을 통해 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.

OpenShift 고려 사항

- 클러스터 간에 앱을 복제하는 경우 소스 클러스터와 대상 클러스터는 OpenShift의 배포 환경과 동일해야 합니다. 예를 들어 OpenShift 4.7 클러스터에서 앱을 클론하는 경우 OpenShift 4.7인 대상 클러스터를 사용합니다.
- OpenShift 클러스터에서 앱을 호스팅하기 위한 프로젝트를 만들면 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. * 클론 세부 정보 *: 클론에 대한 세부 정보 지정:
   - 이름을 입력합니다.
   - 클론의 네임스페이스를 입력합니다.
   - 클론의 대상 클러스터를 선택합니다.
   - 기존 스냅샷이나 백업에서 클론을 생성할지 여부를 선택합니다. 이 옵션을 선택하지 않으면 Astra Control Center는 앱의 현재 상태에서 클론을 생성합니다.

5. * 소스 *: 기존 스냅샷 또는 백업에서 복제하도록 선택한 경우 사용할 스냅샷 또는 백업을 선택합니다.
6. Review * 를 선택합니다.
7. * 클론 요약 *: 클론에 대한 세부 정보를 검토하고 * 클론 * 을 선택합니다.

결과

Astra Control Center는 사용자가 제공한 정보를 기반으로 해당 앱을 복제합니다. 새 애플리케이션 클론이 에 있을 때 클론 작업이 성공적으로 수행됩니다 `Available` 상태를 표시합니다.

> 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.

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 Control은 실행 가능 시점을 기준으로 다음과 같은 유형의 실행 후크를 지원합니다.

- 사전 스냅샷
- 사후 스냅샷
- 사전 백업
- 백업 후
- 사후 복원

사용자 정의 실행 후크에 대한 중요 참고 사항

앱에 대한 실행 후크를 계획할 때 다음 사항을 고려하십시오.

- 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).

> 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 후크는 백업이 완료된 것으로 가정할 수 없습니다.

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, 5가지 유형의 후크가 모두 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
1	복제	해당 없음	해당 없음	신규	동일합니다	예	해당 없음	예
2	복제	해당 없음	해당 없음	신규	다릅니다	예	예	예
3	복제 또는 복원	예	해당 없음	신규	동일합니다	해당 없음	해당 없음	예
4	복제 또는 복원	해당 없음	예	신규	동일합니다	해당 없음	해당 없음	예
5	복제 또는 복원	예	해당 없음	신규	다릅니다	해당 없음	예	예
6	복제 또는 복원	해당 없음	예	신규	다릅니다	해당 없음	해당 없음	예
7	복원	예	해당 없음	기존	동일합니다	해당 없음	해당 없음	예
8	복원	해당 없음	예	기존	동일합니다	해당 없음	해당 없음	예
9	스냅샷	해당 없음	해당 없음	해당 없음	해당 없음	예	해당 없음	해당 없음
10	백업	해당 없음	해당 없음	해당 없음	해당 없음	예	예	해당 없음
11	백업	예	해당 없음	해당 없음	해당 없음	해당 없음	예	해당 없음

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, 소스 및 실행 시간(사전 또는 사후 작업)을 확인할 수 있습니다. 실행 후크를 둘러싼 이벤트 로그를 보려면 왼쪽 탐색 영역의 * Activity * 페이지로 이동합니다.

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

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. 계정 * 으로 이동합니다.
2. 스크립트 * 탭을 선택합니다.
3. 추가 * 를 선택합니다.
4. 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.
5. 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

앱의 사용자 정의 실행 후크를 만들 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. 응용 프로그램 * 을 선택한 다음 관리되는 응용 프로그램의 이름을 선택합니다.
2. Execution hook * 탭을 선택합니다.
3. 추가 * 를 선택합니다.
4. Hook Details * (후크 세부 정보 *) 영역에서 * Operation * (작업 *) 드롭다운 메뉴에서 작업 유형을 선택하여 후크를 실행할 시기를 결정합니다.
5. 후크의 고유한 이름을 입력합니다.
6. (선택 사항) 실행 중에 후크에 전달할 인수를 입력하고 각 인수 뒤에 Enter 키를 눌러 각 인수를 기록합니다.
7. Container Images * (컨테이너 이미지 *) 영역에서 응용 프로그램에 포함된 모든 컨테이너 이미지에 대해 후크를 실행해야 하는 경우 * Apply to all container images * (모든 컨테이너 이미지에 적용) 확인란을 활성화합니다. 대신 후크가 하나 이상의 지정된 컨테이너 이미지에만 동작해야 하는 경우 일치시킬 * 컨테이너 이미지 이름 필드에 컨테이너 이미지 이름을 입력합니다.
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. 후크 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 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.

실행 후크 예

다음 예제를 사용하여 실행 후크를 구조화하는 방법에 대해 알아보십시오. 이러한 후크를 템플릿 또는 테스트 스크립트로 사용할 수 있습니다.

간단한 성공 사례

다음은 표준 출력 및 표준 오류에 성공하여 메시지를 기록하는 간단한 후크의 예입니다.

```
#!/bin/sh

# success_sample.sh
#
# A simple noop success hook script for testing purposes.
#
# args: None
#



#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}



#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
```

```
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running success_sample.sh"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

단순한 성공 사례(bash 버전)

다음은 bash용으로 작성된 표준 출력 및 표준 오류에 성공하여 메시지를 쓰는 간단한 후크의 예입니다.

```
#!/bin/bash

# success_sample.bash
#
# A simple noop success hook script for testing purposes.
#
# args: None


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}
```

```
#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running success_sample.bash"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

간단한 성공 사례**(zsh** 버전**)**

다음은 Z 셸에 대해 작성된 표준 출력 및 표준 오류에 성공하여 메시지를 기록하는 간단한 후크의 예입니다.

```
#!/bin/zsh

# success_sample.zsh
#
# A simple noop success hook script for testing purposes.
#
# args: None
#


#
```

```
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}

#
# main
#

# log something to stdout
info "running success_sample.zsh"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

인수 성공 예제

다음 예제에서는 후크에 args를 사용하는 방법을 보여 줍니다.

```
#!/bin/sh

# success_sample_args.sh
#
```

```
# A simple success hook script with args for testing purposes.
#
# args: Up to two optional args that are echoed to stdout

#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running success_sample_args.sh"


# collect args
arg1=$1
arg2=$2

# output args and arg count to stdout
info "number of args: $#"
```

```
info "arg1 ${arg1}"
info "arg2 ${arg2}"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

사전 스냅샷/사후 스냅샷 후크의 예

다음 예제에서는 사전 스냅샷 및 사후 스냅샷 후크에 대해 동일한 스크립트를 사용하는 방법을 보여 줍니다.

```
#!/bin/sh

# success_sample_pre_post.sh
#
# A simple success hook script example with an arg for testing purposes
# to demonstrate how the same script can be used for both a prehook and
posthook
#
# args: [pre|post]

# unique error codes for every error case
ebase=100
eusage=$((ebase+1))
ebadstage=$((ebase+2))
epre=$((ebase+3))
epost=$((ebase+4))



#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}



#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
```

```
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# Would run prehook steps here
#
prehook() {
    info "Running noop prehook"
    return 0
}

#
# Would run posthook steps here
#
posthook() {
    info "Running noop posthook"
    return 0
}


#
# main
#

# check arg
stage=$1
if [ -z "${stage}" ]; then
    echo "Usage: $0 <pre|post>"
    exit ${eusage}
fi

if [ "${stage}" != "pre" ] && [ "${stage}" != "post" ]; then
    echo "Invalid arg: ${stage}"
    exit ${ebadstage}
fi

# log something to stdout
```

```
info "running success_sample_pre_post.sh"

if [ "${stage}" = "pre" ]; then
    prehook
    rc=$?
    if [ ${rc} -ne 0 ]; then
        error "Error during prehook"
    fi
fi

if [ "${stage}" = "post" ]; then
    posthook
    rc=$?
    if [ ${rc} -ne 0 ]; then
        error "Error during posthook"
    fi
fi

exit ${rc}
```

실패 예

다음 예제에서는 후크의 장애를 처리하는 방법을 보여 줍니다.

```
#!/bin/sh

# failure_sample_arg_exit_code.sh
#
# A simple failure hook script for testing purposes.
#
# args: [the exit code to return]
#



#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}



#
# Writes the given information message to standard output
```

```
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running failure_sample_arg_exit_code.sh"

argexitcode=$1

# log to stderr
error "script failed, returning exit code ${argexitcode}"

# exit with specified exit code
exit ${argexitcode}
```

자세한 정보 표시 실패 예

다음 예제에서는 더 자세한 정보 로깅을 사용하여 후크의 오류를 처리하는 방법을 보여 줍니다.

```
#!/bin/sh

# failure_sample_verbose.sh
#
# A simple failure hook script with args for testing purposes.
#
# args: [The number of lines to output to stdout]


#
```

```
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running failure_sample_verbose.sh"


# output arg value to stdout
linecount=$1
info "line count ${linecount}"

# write out a line to stdout based on line count arg
i=1
while [ "$i" -le ${linecount} ]; do
    info "This is line ${i} from failure_sample_verbose.sh"
    i=$(( i + 1 ))
done
```

```
error "exiting with error code 8"
exit 8
```

종료 코드 예제에 오류가 발생했습니다

다음 예제에서는 종료 코드와 함께 후크 실패를 보여 줍니다.

```
#!/bin/sh

# failure_sample_arg_exit_code.sh
#
# A simple failure hook script for testing purposes.
#
# args: [the exit code to return]
#



#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}



#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}
```

```
#
# main
#

# log something to stdout
info "running failure_sample_arg_exit_code.sh"

argexitcode=$1

# log to stderr
error "script failed, returning exit code ${argexitcode}"

# exit with specified exit code
exit ${argexitcode}
```

실패 후 성공 예

다음 예제에서는 후크가 처음 실행될 때 후크가 실패하지만 두 번째 실행 후에 후크가 발생하는 방법을 보여 줍니다.

```
#!/bin/sh

# failure_then_success_sample.sh
#
# A hook script that fails on initial run but succeeds on second run for
testing purposes.
#
# Helpful for testing retry logic for post hooks.
#
# args: None
#

#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}



#
# Writes the given information message to standard output
#
# $* - The message to write
#
```

```
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running failure_success sample.sh"


if [ -e /tmp/hook-test.junk ] ; then
    info "File does exist.  Removing /tmp/hook-test.junk"
    rm /tmp/hook-test.junk
    info "Second run so returning exit code 0"
    exit 0
else
    info "File does not exist.  Creating /tmp/hook-test.junk"
    echo "test" > /tmp/hook-test.junk
    error "Failed first run, returning exit code 5"
    exit 5
fi
```

앱 및 클러스터 상태를 모니터링합니다

앱 및 클러스터 상태 요약 보기

대시보드 * 를 선택하면 앱, 클러스터, 스토리지 백엔드 및 상태를 한눈에 파악할 수 있습니다.

이것들은 단순히 정적 숫자나 상태만이 아니라, 각 상태로부터 드릴다운할 수 있습니다. 예를 들어 앱이 완전히 보호되지 않은 경우 아이콘 위로 마우스를 가져가면 완전히 보호되지 않은 앱을 확인할 수 있습니다. 여기에는 이유가 포함됩니다.

응용 프로그램 타일

응용 프로그램* 타일은 다음 사항을 식별하는 데 도움이 됩니다.

- 현재 관리 중인 애플리케이션 수는 Astra입니다.
- 관리된 앱이 정상 상태인지 여부
- 애플리케이션이 완전히 보호되는지 여부(최근 백업을 사용할 수 있는 경우 보호됨)
- 검색되었지만 아직 관리되지 않은 앱의 수입니다.

  앱을 검색한 후 관리하거나 무시하면 되므로 이 숫자는 0이 되는 것이 좋습니다. 그런 다음 대시보드에서 검색된 앱의 수를 모니터링하여 개발자가 클러스터에 새 앱을 추가하는 시기를 파악할 수 있습니다.

클러스터 타일

클러스터 * 타일은 Astra Control Center를 사용하여 관리하고 있는 클러스터의 상태에 대한 유사한 세부 정보를 제공하며, 앱을 사용하는 것처럼 드릴다운하여 더 자세한 정보를 얻을 수 있습니다.

저장소 백엔드 타일

저장소 백엔드 * 타일은 다음을 포함하여 저장소 백엔드의 상태를 식별하는 데 도움이 되는 정보를 제공합니다.

- 관리되는 스토리지 백엔드 수
- 이러한 관리되는 백엔드가 정상 상태인지 여부
- 백엔드가 완전히 보호되는지 여부
- 검색되었지만 아직 관리되지 않은 백엔드 수입니다.

클러스터의 상태 및 세부 정보를 봅니다

Astra Control Center에서 관리할 클러스터를 추가한 후에는 클러스터의 위치, 작업자 노드, 영구 볼륨 및 스토리지 클래스 등의 클러스터에 대한 세부 정보를 볼 수 있습니다.

단계

1. Astra Control Center UI에서 * Clusters * 를 선택합니다.
2. 클러스터 * 페이지에서 세부 정보를 확인할 클러스터를 선택합니다.

   > 클러스터가 인 경우 `removed` 클러스터 및 네트워크 연결이 양호해 보이지만(Kubernetes API를 사용하여 클러스터에 액세스하려는 외부 시도가 성공한 경우), Astra Control에 제공한 kubeconfig는 더 이상 유효하지 않을 수 있습니다. 클러스터의 인증서 순환 또는 만료 때문일 수 있습니다. 이 문제를 해결하려면 을 사용하여 Astra Control의 클러스터와 연결된 자격 증명을 업데이트하십시오 "Astra Control API를 참조하십시오".

3. Overview *, * Storage * 및 * Activity * 탭에서 원하는 정보를 확인할 수 있습니다.
   - * 개요 *: 해당 상태를 포함한 작업자 노드에 대한 세부 정보.
   - * 스토리지 *: 스토리지 클래스 및 상태를 비롯하여 컴퓨팅과 연관된 영구 볼륨입니다.
   - * Activity *: 클러스터와 관련된 활동을 표시합니다.

Astra Control Center * 대시보드 * 부터 클러스터 정보를 볼 수도 있습니다. 리소스 요약 * 의 * 클러스터 * 탭에서 * 클러스터 * 페이지로 이동하는 관리 클러스터를 선택할 수 있습니다. 클러스터 * 페이지로 이동한 후 위에 설명된 단계를 따릅니다.

앱의 상태 및 세부 정보를 봅니다

앱 관리를 시작한 후 Astra는 앱의 상태(정상 여부), 보호 상태(장애 시 완전히 보호되는지 여부), Pod, 영구 스토리지 등을 식별할 수 있는 앱에 대한 세부 정보를 제공합니다.

단계

1. Astra Control Center UI에서 * 응용 프로그램 * 을 선택한 다음 앱 이름을 선택합니다.
2. 원하는 정보를 찾습니다.

앱 상태

Kubernetes의 앱 상태를 반영하는 상태를 제공합니다. 예를 들어, Pod와 영구 볼륨을 온라인으로 전환합니까? 앱이 정상 상태가 아닌 경우 Kubernetes 로그를 확인하여 클러스터에서 문제를 해결해야 합니다. Astra는 고장난 앱을 수정하는 데 도움이 되는 정보를 제공하지 않습니다.

앱 보호 상태

앱이 얼마나 잘 보호되는지 상태를 제공합니다.

- * 완전 보호 *: 이 앱에는 활성 백업 스케줄과 1주일 미만의 성공적인 백업이 있습니다
- * 부분 보호됨 *: 응용 프로그램에 활성 백업 일정, 활성 스냅샷 일정 또는 백업 또는 스냅샷이 있습니다
- * 보호되지 않음 *: 완전히 보호되거나 부분적으로 보호되지 않는 앱

  _최근 백업 _ 이(가) 있을 때까지 완전히 보호할 수 없습니다. 백업은 영구 볼륨으로부터 멀리 떨어진 개체 저장소에 저장되기 때문에 이 작업이 중요합니다. 장애 또는 사고로 인해 클러스터가 삭제되며 영구적 저장소인 경우 복구할 백업이 필요합니다. 스냅샷을 사용하면 복구할 수 없습니다.

개요

앱과 연결된 Pod의 상태에 대한 정보입니다.

데이터 보호

데이터 보호 정책을 구성하고 기존 스냅샷 및 백업을 볼 수 있습니다.

스토리지

에는 애플리케이션 레벨의 영구 볼륨이 나와 있습니다. 영구 볼륨의 상태는 Kubernetes 클러스터의 관점에서 나옵니다.

리소스

백업 및 관리되는 리소스를 확인할 수 있습니다.

활동입니다

앱 관련 활동을 보여줍니다.

Astra Control Center * Dashboard * 부터 앱 정보를 볼 수도 있습니다. 리소스 요약 * 의 * 응용 프로그램 * 탭에서 * 응용 프로그램 * 페이지로 이동하는 관리되는 앱을 선택할 수 있습니다. 응용 프로그램 * 페이지로 이동한 후 위에 설명된 단계를 따릅니다.

계정을 관리합니다

사용자 관리

Astra Control Center 설치 사용자를 Astra Control UI를 사용하여 초대, 추가, 제거 및 편집할 수 있습니다. Astra Control UI 또는 를 사용할 수 있습니다 "Astra Control API" 를 눌러 사용자를 관리합니다.

LDAP를 사용하여 선택한 사용자에 대한 인증을 수행할 수도 있습니다.

LDAP를 사용합니다

LDAP는 분산된 디렉터리 정보에 액세스하기 위한 업계 표준 프로토콜이며 엔터프라이즈 인증에 널리 사용되는 프로토콜입니다. Astra Control Center를 LDAP 서버에 연결하여 선택한 Astra 사용자에 대한 인증을 수행할 수 있습니다. 이 구성에는 Astra와 LDAP를 통합하고 LDAP 정의에 해당하는 Astra 사용자 및 그룹을 정의하는 작업이 포함됩니다. 을 참조하십시오 "LDAP 인증" 를 참조하십시오.

사용자를 초대합니다

계정 소유자와 관리자는 새 사용자를 Astra Control Center에 초대할 수 있습니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 사용자 * 탭을 선택합니다.
3. 사용자 초대 * 를 선택합니다.
4. 사용자의 이름과 이메일 주소를 입력합니다.
5. 적절한 시스템 권한이 있는 사용자 역할을 선택합니다.

   각 역할은 다음과 같은 권한을 제공합니다.

   - Viewer * 는 리소스를 볼 수 있습니다.
   - 구성원 * 은 뷰어 역할 권한을 가지며 앱 및 클러스터를 관리하고, 앱을 관리하고, 스냅샷 및 백업을 삭제할 수 있습니다.
   - Admin * 은 구성원 역할 권한을 가지며 소유자를 제외한 다른 사용자를 추가 및 제거할 수 있습니다.
   - 소유자 * 는 관리자 역할 권한을 가지며 모든 사용자 계정을 추가 및 제거할 수 있습니다.
6. 멤버 또는 뷰어 역할이 있는 사용자에게 제약 조건을 추가하려면 * 제약 조건으로 역할 제한 * 확인란을 활성화합니다.

   제약 조건 추가에 대한 자세한 내용은 을 참조하십시오 "역할을 관리합니다".

7. 사용자 초대 * 를 선택합니다.

   사용자에게 Astra Control Center에 초대되었음을 알리는 이메일이 전송됩니다. 이 이메일에는 임시 암호가

포함되어 있으며, 이 암호는 처음 로그인할 때 변경해야 합니다.

사용자 추가

계정 소유자와 관리자는 Astra Control Center 설치에 사용자를 더 추가할 수 있습니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 사용자 * 탭을 선택합니다.
3. 사용자 추가 * 를 선택합니다.
4. 사용자 이름, 이메일 주소 및 임시 암호를 입력합니다.

   사용자는 처음 로그인할 때 암호를 변경해야 합니다.

5. 적절한 시스템 권한이 있는 사용자 역할을 선택합니다.

   각 역할은 다음과 같은 권한을 제공합니다.

   - Viewer * 는 리소스를 볼 수 있습니다.
   - 구성원 * 은 뷰어 역할 권한을 가지며 앱 및 클러스터를 관리하고, 앱을 관리하고, 스냅샷 및 백업을 삭제할 수 있습니다.
   - Admin * 은 구성원 역할 권한을 가지며 소유자를 제외한 다른 사용자를 추가 및 제거할 수 있습니다.
   - 소유자 * 는 관리자 역할 권한을 가지며 모든 사용자 계정을 추가 및 제거할 수 있습니다.

6. 멤버 또는 뷰어 역할이 있는 사용자에게 제약 조건을 추가하려면 * 제약 조건으로 역할 제한 * 확인란을 활성화합니다.

   제약 조건 추가에 대한 자세한 내용은 을 참조하십시오 "역할을 관리합니다".

7. 추가 * 를 선택합니다.

암호 관리

Astra Control Center에서 사용자 계정의 암호를 관리할 수 있습니다.

암호를 변경합니다

언제든지 사용자 계정의 암호를 변경할 수 있습니다.

단계

1. 화면 오른쪽 상단에서 사용자 아이콘을 선택합니다.
2. 프로파일 * 을 선택합니다.
3. 작업 * 열의 옵션 메뉴에서 * 암호 변경 * 을 선택합니다.
4. 암호 요구 사항에 맞는 암호를 입력합니다.
5. 암호를 다시 입력하여 확인합니다.
6. 암호 변경 * 을 선택합니다.

다른 사용자의 암호를 재설정합니다

계정에 관리자 또는 소유자 역할 권한이 있는 경우 다른 사용자 계정과 사용자의 암호를 재설정할 수 있습니다. 암호를 재설정할 때 사용자가 로그인할 때 변경해야 하는 임시 암호를 할당합니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 작업 * 드롭다운 목록을 선택합니다.
3. 암호 재설정 * 을 선택합니다.
4. 암호 요구 사항에 맞는 임시 암호를 입력합니다.
5. 암호를 다시 입력하여 확인합니다.

   다음에 사용자가 로그인할 때 암호를 변경하라는 메시지가 표시됩니다.

6. 비밀번호 재설정 * 을 선택합니다.

사용자의 역할을 변경합니다

소유자 역할을 가진 사용자는 모든 사용자의 역할을 변경할 수 있지만 관리자 역할을 가진 사용자는 관리자, 구성원 또는 뷰어 역할을 가진 사용자의 역할을 변경할 수 있습니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 작업 * 드롭다운 목록을 선택합니다.
3. 역할 편집 * 을 선택합니다.
4. 새 역할을 선택합니다.
5. 역할에 제약 조건을 적용하려면 * 제약 조건으로 역할 제한 * 확인란을 선택하고 목록에서 제약 조건을 선택합니다.

   구속조건이 없으면 구속조건을 추가할 수 있습니다. 자세한 내용은 을 참조하십시오 "역할을 관리합니다".

6. Confirm * 을 선택합니다.

결과

Astra Control Center는 선택한 새 역할에 따라 사용자의 권한을 업데이트합니다.

사용자를 제거합니다

소유자 또는 관리자 역할을 가진 사용자는 언제든지 계정에서 다른 사용자를 제거할 수 있습니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 사용자 * 탭에서 제거할 각 사용자의 행에서 확인란을 선택합니다.
3. Actions * 열의 Options 메뉴에서 * Remove user/s * 를 선택합니다.
4. 메시지가 표시되면 "remove(제거)"라는 단어를 입력한 다음 * Yes, Remove User(예, 사용자 제거) * 를 선택하여 삭제를 확인합니다.

결과

Astra Control Center는 계정에서 사용자를 제거합니다.

역할을 관리합니다

네임스페이스 제약 조건을 추가하고 이러한 제약 조건에 대한 사용자 역할을 제한하여 역할을 관리할 수 있습니다. 이렇게 하면 조직 내의 리소스에 대한 액세스를 제어할 수 있습니다. Astra Control UI 또는 를 사용할 수 있습니다 "Astra Control API" 역할을 관리합니다.

역할에 네임스페이스 제약 조건을 추가합니다

관리자 또는 소유자 사용자는 네임스페이스 제약 조건을 추가할 수 있습니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 사용자 * 탭을 선택합니다.
3. Actions * 열에서 Member 또는 Viewer 역할을 가진 사용자의 메뉴 버튼을 선택합니다.
4. 역할 편집 * 을 선택합니다.
5. 제약 조건으로 역할 제한 * 확인란을 활성화합니다.

   이 확인란은 구성원 또는 뷰어 역할에만 사용할 수 있습니다. 역할 * 드롭다운 목록에서 다른 역할을 선택할 수 있습니다.

6. 구속 조건 추가 * 를 선택합니다.

   네임스페이스 또는 네임스페이스 레이블별로 사용 가능한 제약 조건 목록을 볼 수 있습니다.

7. 네임스페이스 구성 방법에 따라 * 제약 조건 유형 * 드롭다운 목록에서 * Kubernetes 네임스페이스 * 또는 * Kubernetes 네임스페이스 레이블 * 을 선택합니다.
8. 목록에서 하나 이상의 네임스페이스 또는 레이블을 선택하여 해당 네임스페이스로 역할을 제한하는 제약 조건을 구성합니다.
9. Confirm * 을 선택합니다.

   역할 편집 * 페이지에는 이 역할에 대해 선택한 제약 조건 목록이 표시됩니다.

10. Confirm * 을 선택합니다.

    계정 * 페이지의 * 역할 * 열에서 구성원 또는 뷰어 역할에 대한 제약 조건을 볼 수 있습니다.

> 역할에 대한 제약 조건을 설정하고 제약 조건을 추가하지 않고 * 확인 * 을 선택하면 역할이 전체 제한 사항으로 간주됩니다(역할에 네임스페이스가 할당된 리소스에 대한 액세스가 거부됨).

역할에서 네임스페이스 제약 조건을 제거합니다

관리자 또는 소유자 사용자는 역할에서 네임스페이스 제약 조건을 제거할 수 있습니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 사용자 * 탭을 선택합니다.
3. Actions * 열에서 활성 제약 조건이 있는 Member 또는 Viewer 역할을 가진 사용자의 메뉴 버튼을 선택합니다.
4. 역할 편집 * 을 선택합니다.

   역할 편집 * 대화 상자에 해당 역할에 대한 활성 제약 조건이 표시됩니다.

5. 제거할 구속 조건의 오른쪽에 있는 * X * 를 선택합니다.
6. Confirm * 을 선택합니다.

를 참조하십시오

- "사용자 역할 및 네임스페이스"

알림을 보고 관리합니다

Astra는 작업이 완료되거나 실패했을 때 알려줍니다. 예를 들어, 앱 백업이 성공적으로 완료되면 알림이 표시됩니다.

인터페이스의 오른쪽 상단에서 이러한 알림을 관리할 수 있습니다.

단계

1. 오른쪽 상단에서 읽지 않은 알림 수를 선택합니다.
2. 알림을 검토한 후 * 읽은 상태로 표시 * 또는 * 모든 알림 표시 * 를 선택합니다.

   모든 알림 표시 * 를 선택한 경우 알림 페이지가 로드됩니다.

3. 알림 * 페이지에서 알림을 보고 읽음으로 표시할 알림을 선택하고 * 작업 * 을 선택한 다음 * 읽음으로 표시 * 를 선택합니다.

자격 증명을 추가 및 제거합니다

ONTAP S3, OpenShift로 관리되는 Kubernetes 클러스터, 또는 관리되지 않는 Kubernetes 클러스터와 같은 로컬 프라이빗 클라우드 공급자의 자격 증명을 언제든지 계정에서 추가 및 제거할 수 있습니다. Astra Control Center는 이러한 자격 증명을 사용하여 Kubernetes 클러스터 및 클러스터의 앱을 검색하고 대신 리소스를 프로비저닝합니다.

Astra Control Center의 모든 사용자는 동일한 자격 증명 세트를 공유합니다.

자격 증명을 추가합니다

클러스터를 관리할 때 Astra Control Center에 자격 증명을 추가할 수 있습니다. 새 클러스터를 추가하여 자격 증명을 추가하려면 을 참조하십시오 "Kubernetes 클러스터 추가".

> 직접 만드는 경우 `kubeconfig` 파일에서 * 하나의 * 컨텍스트 요소만 정의해야 합니다. 을 참조하십시오 "Kubernetes 문서" 을 참조하십시오 `kubeconfig` 파일.

자격 증명을 제거합니다

언제든지 계정에서 자격 증명을 제거합니다. 자격 증명은 이후에 제거해야 합니다 "연결된 모든 클러스터의 관리를 취소합니다".

> Astra Control Center에 추가하는 첫 번째 자격 증명 세트는 항상 사용 중입니다. Astra Control Center는 자격 증명을 사용하여 백업 버킷에 인증하기 때문입니다. 이러한 자격 증명을 제거하지 않는 것이 좋습니다.

단계

1. 계정 * 을 선택합니다.
2. 자격 증명 * 탭을 선택합니다.
3. 제거할 자격 증명에 대한 * 상태 * 열의 옵션 메뉴를 선택합니다.
4. 제거 * 를 선택합니다.
5. 삭제를 확인하려면 "remove(제거)"라는 단어를 입력한 다음 * Yes(예), Remove Credential(자격 증명 제거) * 을 선택합니다.

결과

Astra Control Center는 계정에서 자격 증명을 제거합니다.

계정 활동을 모니터링합니다

Astra Control 계정의 활동에 대한 세부 정보를 볼 수 있습니다. 예를 들어, 새 사용자를 초대하거나, 클러스터를 추가하거나, 스냅샷을 생성할 때 사용할 수 있습니다. 계정 활동을 CSV 파일로 내보낼 수도 있습니다.

> Astra Control에서 Kubernetes 클러스터를 관리하고, Astra Control이 Cloud Insights에 연결된 경우, Astra Control은 이벤트 로그를 Cloud Insights로 보냅니다. POD 배포 및 PVC 첨부 파일에 대한 정보를 포함한 로그 정보가 Astra Control Activity 로그에 표시됩니다. 이 정보를 사용하여 관리하고 있는 Kubernetes 클러스터의 문제를 식별할 수 있습니다.

Astra Control에서 모든 계정 활동을 봅니다

1. Activity * 를 선택합니다.
2. 필터를 사용하여 활동 목록의 범위를 좁히거나 검색 상자를 사용하여 원하는 항목을 정확하게 찾을 수 있습니다.
3. CSV로 내보내기 * 를 선택하여 계정 활동을 CSV 파일로 다운로드합니다.

특정 앱의 계정 활동을 봅니다

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

클러스터의 계정 활동을 봅니다

1. 클러스터 * 를 선택한 다음 클러스터 이름을 선택합니다.
2. Activity * 를 선택합니다.

주의가 필요한 이벤트를 해결하기 위한 조치를 취하십시오

1. Activity * 를 선택합니다.
2. 주의가 필요한 이벤트를 선택합니다.
3. 실행 * 드롭다운 옵션을 선택합니다.

   이 목록에서 수행할 수 있는 수정 조치를 확인하고, 문제와 관련된 문서를 보고, 문제 해결을 위한 지원을 받을 수 있습니다.

기존 라이센스를 업데이트합니다

평가판 라이센스를 전체 라이센스로 변환하거나 기존 평가판 또는 전체 라이센스를 새 라이센스로 업데이트할 수 있습니다. 전체 라이센스가 없는 경우 NetApp 세일즈 담당자와 협력하여 전체 라이센스 및 일련 번호를 받으십시오. Astra UI 또는 를 사용할 수 있습니다 "Astra Control API" 기존 라이센스를 업데이트합니다.

단계

1. 에 로그인합니다 "NetApp Support 사이트".
2. Astra Control Center 다운로드 페이지에 액세스하여 일련 번호를 입력한 다음 전체 NetApp 라이센스 파일(NLF)을 다운로드하십시오.
3. Astra Control Center UI에 로그인합니다.
4. 왼쪽 탐색 창에서 * 계정 * > * 라이센스 * 를 선택합니다.
5. 계정 * > * 라이선스 * 페이지에서 기존 라이선스의 상태 드롭다운 메뉴를 선택하고 * 교체 * 를 선택합니다.
6. 다운로드한 라이센스 파일을 찾습니다.
7. 추가 * 를 선택합니다.

Account * > * Licenses * 페이지에는 라이센스 정보, 만료 날짜, 라이센스 일련 번호, 계정 ID 및 사용된 CPU 단위가 표시됩니다.

를 참조하십시오

- "Astra Control Center 라이센스"

리포지토리 연결을 관리합니다

저장소를 Astra Control에 연결하여 소프트웨어 패키지 설치 이미지 및 아티팩트에 대한 참조로 사용할 수 있습니다. 소프트웨어 패키지를 가져올 때 Astra Control은 이미지 리포지토리의 설치 이미지 및 바이너리 및 기타 아티팩트의 아티팩트를 참조합니다.

필요한 것

- Astra Control Center가 설치된 Kubernetes 클러스터
- 액세스할 수 있는 실행 중인 Docker 리포지토리입니다
- 액세스할 수 있는 실행 아티팩트 저장소(예: Artifactory)

Docker 이미지 저장소를 연결합니다

Docker 이미지 저장소를 연결하여 Astra Data Store와 같은 패키지 설치 이미지를 보관할 수 있습니다. 패키지를 설치할 때 Astra Control은 이미지 저장소에서 패키지 이미지 파일을 가져옵니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 연결 * 탭을 선택합니다.
3. Docker Image Repository * 섹션에서 오른쪽 상단의 메뉴를 선택합니다.
4. Connect * 를 선택합니다.
5. 리포지토리의 URL 및 포트를 추가합니다.
6. 리포지토리의 자격 증명을 입력합니다.
7. Connect * 를 선택합니다.

결과

리포지토리가 연결되었습니다. Docker Image Repository * 섹션에서 리포지토리가 연결됨 상태를 표시해야 합니다.

Docker 이미지 리포지토리 연결을 끊습니다

더 이상 필요하지 않은 경우 Docker 이미지 저장소에 대한 연결을 제거할 수 있습니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 연결 * 탭을 선택합니다.
3. Docker Image Repository * 섹션에서 오른쪽 상단의 메뉴를 선택합니다.
4. Disconnect * 를 선택합니다.
5. 예, Docker 이미지 리포지토리 * 를 연결 해제합니다.

결과

리포지토리의 연결이 끊겼습니다. Docker Image Repository * 섹션에서 리포지토리의 연결 끊김 상태가 표시되어야 합니다.

아티팩트 리포지토리를 연결합니다

아티팩트 리포지토리를 소프트웨어 패키지 바이너리와 같은 호스트 아티팩트에 연결할 수 있습니다. 패키지를 설치할 때 Astra Control은 이미지 저장소에서 소프트웨어 패키지에 대한 아티팩트를 가져옵니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 연결 * 탭을 선택합니다.
3. Artifact Repository * 섹션에서 오른쪽 상단의 메뉴를 선택합니다.
4. Connect * 를 선택합니다.
5. 리포지토리의 URL 및 포트를 추가합니다.

6. 인증이 필요한 경우 * Use authentication *(인증 사용 *) 확인란을 선택하고 리포지토리의 자격 증명을 입력합니다.
7. Connect * 를 선택합니다.

결과

리포지토리가 연결되었습니다. Artifact Repository * 섹션에서 리포지토리는 연결된 상태를 표시해야 합니다.

아티팩트 저장소의 연결을 해제합니다

더 이상 필요하지 않은 경우 아티팩트 리포지토리에 대한 연결을 제거할 수 있습니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 연결 * 탭을 선택합니다.
3. Artifact Repository * 섹션에서 오른쪽 상단의 메뉴를 선택합니다.
4. Disconnect * 를 선택합니다.
5. Yes, disconnect artifact repository * 를 선택합니다.

결과

리포지토리의 연결이 끊겼습니다. Artifact Repository * 섹션에서 리포지토리는 연결된 상태를 표시해야 합니다.

자세한 내용을 확인하십시오

- "소프트웨어 패키지를 관리합니다"

소프트웨어 패키지를 관리합니다

NetApp은 NetApp Support 사이트에서 다운로드할 수 있는 소프트웨어 패키지가 포함된 Astra Control Center에 대한 추가 기능을 제공합니다. Docker 및 아티팩트 저장소를 연결한 후 패키지를 업로드 및 가져와 Astra Control Center에 이 기능을 추가할 수 있습니다. CLI 또는 Astra Control Center 웹 UI를 사용하여 소프트웨어 패키지를 관리할 수 있습니다.

필요한 것

- Astra Control Center가 설치된 Kubernetes 클러스터
- 소프트웨어 패키지 이미지를 보관할 연결된 Docker 이미지 리포지토리입니다. 자세한 내용은 을 참조하십시오 "리포지토리 연결을 관리합니다".
- 소프트웨어 패키지 바이너리 및 아티팩트를 보관하는 연결된 아티팩트 리포지토리입니다. 자세한 내용은 을 참조하십시오 "리포지토리 연결을 관리합니다".
- NetApp Support 사이트의 소프트웨어 패키지입니다

소프트웨어 패키지 이미지를 리포지토리에 업로드합니다

Astra Control Center는 연결된 저장소의 패키지 이미지 및 아티팩트를 참조합니다. CLI를 사용하여 이미지 및 아티팩트를 리포지토리에 업로드할 수 있습니다.

단계

1. NetApp Support 사이트에서 소프트웨어 패키지를 다운로드하여 가 있는 컴퓨터에 저장합니다 `kubectl`

유틸리티가 설치되었습니다.

2. 압축된 패키지 파일의 압축을 풀고 디렉토리를 Astra Control 번들 파일의 위치로 변경합니다(예: `acc.manifest.yaml`)를 클릭합니다.
3. 패키지 이미지를 Docker 저장소로 푸시합니다. 다음 대체 작업을 수행합니다.
   - Bundle_file을 Astra Control 번들 파일 이름으로 바꿉니다(예: `acc.manifest.yaml`)를 클릭합니다.
   - my_registry를 Docker 리포지토리의 URL로 바꿉니다.
   - my_registry_user를 사용자 이름으로 바꿉니다.
   - my_registry_token을 레지스트리에 대한 인증된 토큰으로 바꿉니다.

   ```
   kubectl astra packages push-images -m BUNDLE_FILE -r MY_REGISTRY -u
   MY_REGISTRY_USER -p MY_REGISTRY_TOKEN
   ```

4. 패키지에 아티팩트가 있는 경우 아티팩트를 아티팩트 저장소로 복사합니다. bundle_file을 Astra Control 번들 파일의 이름으로 바꾸고 network_location을 네트워크 위치로 교체하여 다음 위치에 아티팩트 파일을 복사합니다.

   ```
   kubectl astra packages copy-artifacts -m BUNDLE_FILE -n NETWORK_LOCATION
   ```

소프트웨어 패키지를 추가합니다

Astra Control Center 번들 파일을 사용하여 소프트웨어 패키지를 가져올 수 있습니다. 이렇게 하면 패키지가 설치되고 Astra Control Center에서 소프트웨어를 사용할 수 있습니다.

Astra Control 웹 **UI**를 사용하여 소프트웨어 패키지를 추가합니다

Astra Control Center 웹 UI를 사용하여 연결된 저장소에 업로드된 소프트웨어 패키지를 추가할 수 있습니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 패키지 * 탭을 선택합니다.
3. 추가 * 버튼을 선택합니다.
4. 파일 선택 대화 상자에서 업로드 아이콘을 선택합니다.
5. 에서 Astra Control 번들 파일을 선택합니다 `.yaml` 형식, 업로드할 형식.
6. 추가 * 를 선택합니다.

결과

번들 파일이 유효하고 패키지 이미지 및 아티팩트가 연결된 저장소에 있으면 패키지가 Astra Control Center에 추가됩니다. 상태 * 열의 상태가 * 사용 가능 * 으로 변경되면 패키지를 사용할 수 있습니다. 패키지 상태 위로 마우스를 가져가면 추가 정보를 볼 수 있습니다.

> 리포지토리에 패키지에 대한 하나 이상의 이미지 또는 아티팩트가 없으면 해당 패키지에 대한 오류 메시지가 나타납니다.

CLI를 사용하여 소프트웨어 패키지를 추가합니다

CLI를 사용하여 연결된 리포지토리에 업로드한 소프트웨어 패키지를 가져올 수 있습니다. 이를 위해서는 먼저 Astra Control Center 계정 ID와 API 토큰을 기록해야 합니다.

단계

1. 웹 브라우저를 사용하여 Astra Control Center 웹 UI에 로그인합니다.
2. 대시보드에서 오른쪽 상단의 사용자 아이콘을 선택합니다.
3. API 액세스 * 를 선택합니다.
4. 화면 위쪽에 있는 계정 ID를 확인합니다.
5. API 토큰 생성 * 을 선택합니다.
6. 결과 대화 상자에서 * API 토큰 생성 * 을 선택합니다.
7. 결과 토큰을 기록하고 * Close * 를 선택합니다. CLI에서 디렉토리를 의 위치로 변경합니다 `.yaml` 압축을 푼 패키지 내용물의 번들 파일입니다.
8. 번들 파일을 사용하여 패키지를 가져오고 다음 대체 항목을 만듭니다.
   - Bundle_file을 Astra Control 번들 파일의 이름으로 바꿉니다.
   - 서버를 Astra Control 인스턴스의 DNS 이름으로 바꿉니다.
   - account_ID 및 토큰을 이전에 기록한 계정 ID 및 API 토큰으로 교체합니다.

```
kubectl astra packages import -m BUNDLE_FILE -u SERVER -a ACCOUNT_ID
-k TOKEN
```

결과

번들 파일이 유효하고 패키지 이미지 및 아티팩트가 연결된 저장소에 있으면 패키지가 Astra Control Center에 추가됩니다.

> 리포지토리에 패키지에 대한 하나 이상의 이미지 또는 아티팩트가 없으면 해당 패키지에 대한 오류 메시지가 나타납니다.

소프트웨어 패키지를 제거합니다

Astra Control Center 웹 UI를 사용하여 이전에 Astra Control Center에서 가져온 소프트웨어 패키지를 제거할 수 있습니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 패키지 * 탭을 선택합니다.

   이 페이지에서는 설치된 패키지 목록과 해당 상태를 확인할 수 있습니다.

3. 패키지의 * Actions * 열에서 Actions 메뉴를 엽니다.
4. 삭제 * 를 선택합니다.

결과

패키지는 Astra Control Center에서 삭제되지만 패키지의 이미지 및 아티팩트는 저장소에 남아 있습니다.

자세한 내용을 확인하십시오

- "리포지토리 연결을 관리합니다"

버킷을 관리합니다

애플리케이션 및 영구 스토리지를 백업하려는 경우나 클러스터 간에 애플리케이션을 클론 복제하려는 경우에는 오브젝트 저장소 버킷 공급자가 필수적입니다. Astra Control Center를 사용하여 객체 저장소 공급자를 오프라인 클러스터, 앱의 백업 대상으로 추가합니다.

애플리케이션 구성과 영구 스토리지를 동일한 클러스터에 클론 복제할 경우 버킷이 필요하지 않습니다.

다음 Amazon S3(Simple Storage Service) 버킷 공급자 중 하나를 사용하십시오.

- NetApp ONTAP S3
- NetApp StorageGRID S3
- Microsoft Azure를 참조하십시오
- 일반 S3

> AWS(Amazon Web Services) 및 GCP(Google Cloud Platform)는 일반 S3 버킷 유형을 사용합니다.

> Astra Control Center는 Amazon S3를 일반 S3 버킷 공급자로 지원하지만, Astra Control Center는 Amazon의 S3 지원을 주장하는 모든 오브젝트 저장소 공급업체를 지원하지 않을 수 있습니다.

버킷은 다음 상태 중 하나일 수 있습니다.

- 보류 중: 버킷이 검색되도록 예약되었습니다.
- 사용 가능: 버킷을 사용할 수 있습니다.
- 제거: 현재 버킷에 접근할 수 없습니다.

Astra Control API를 사용하여 버킷을 관리하는 방법에 대한 지침은 을 참조하십시오 "Astra 자동화 및 API 정보".

버킷 관리와 관련된 다음 작업을 수행할 수 있습니다.

- "버킷을 추가합니다"
- 버킷을 편집합니다
- 버킷 자격 증명을 회전하거나 제거합니다
- 버킷을 탈거하십시오

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.

버킷을 편집합니다

버킷의 액세스 자격 증명 정보를 변경하고 선택한 버킷이 기본 버킷인지 여부를 변경할 수 있습니다.

버킷을 추가할 때 올바른 버킷 공급자를 선택하고 해당 공급자에 적합한 자격 증명을 제공합니다. 예를 들어, UI에서 NetApp ONTAP S3를 유형으로 받아들이고 StorageGRID 자격 증명을 받아들이지만, 이 버킷을 사용한 이후의 모든 애플리케이션 백업 및 복원이 실패합니다. 를 참조하십시오 "릴리즈 노트".

단계

1. 왼쪽 탐색 창에서 * Bucket * 을 선택합니다.
2. Actions * 열의 Options 메뉴에서 * Edit * 를 선택합니다.
3. 버킷 유형 이외의 모든 정보를 변경합니다.

   버킷 유형을 수정할 수 없습니다.

4. Update * 를 선택합니다.

버킷 자격 증명을 회전하거나 제거합니다

Astra Control은 버킷 자격 증명을 사용하여 액세스 권한을 얻고 S3 버킷에 대한 비밀 키를 제공하여 Astra Control Center가 버킷과 통신할 수 있도록 합니다.

버킷 자격 증명을 회전합니다

자격 증명을 회전하는 경우 백업이 진행 중인 상태(예약 또는 필요 시)가 없을 때 유지 관리 창에서 자격 증명을 회전합니다.

자격 증명을 편집하고 회전하는 단계입니다

1. 왼쪽 탐색 창에서 * Bucket * 을 선택합니다.
2. Actions * 열의 Options 메뉴에서 * Edit * 를 선택합니다.
3. 새 자격 증명을 생성합니다.
4. Update * 를 선택합니다.

버킷 자격 증명을 제거합니다

버킷에 새 자격 증명이 적용된 경우 또는 버킷이 더 이상 사용되지 않는 경우에만 버킷 자격 증명을 제거해야 합니다.

Astra Control에 추가하는 첫 번째 자격 증명 세트는 항상 사용 중입니다. Astra Control은 자격 증명을 사용하여 백업 버킷을 인증하기 때문입니다. 버킷이 사용 중인 경우 이러한 자격 증명을 제거하지 마십시오. 이 경우 백업 실패 및 백업 가용성 손실이 발생할 수 있습니다.

> 활성 버킷 자격 증명을 제거하는 경우 를 참조하십시오 "버킷 자격 증명 제거 문제 해결".

Astra Control API를 사용하여 S3 자격 증명을 제거하는 방법에 대한 지침은 을 참조하십시오 "Astra 자동화 및 API 정보".

버킷을 탈거하십시오

더 이상 사용하지 않거나 상태가 불량한 버킷을 제거할 수 있습니다. 오브젝트 저장소 구성을 단순하고 최신 상태로 유지하기 위해 이 작업을 수행할 수 있습니다.

> 기본 버킷을 제거할 수 없습니다. 해당 버킷을 제거하려면 먼저 다른 버킷을 기본값으로 선택하십시오.

필요한 것

- 시작하기 전에 이 버킷에 대해 실행 중이거나 완료된 백업이 없는지 확인해야 합니다.
- 버킷이 활성 보호 정책에서 사용되고 있지 않은지 확인해야 합니다.

있는 경우 계속할 수 없습니다.

단계

1. 왼쪽 탐색에서 * Bucket * 을 선택합니다.
2. Actions * 메뉴에서 * Remove * 를 선택합니다.

   > Astra Control은 먼저 버킷에 백업을 사용하는 스케줄 정책이 없고 제거할 버킷에 활성 백업이 없음을 보장합니다.

3. 작업을 확인하려면 "remove"를 입력합니다.
4. 예, 버킷 제거 * 를 선택합니다.

자세한 내용을 확인하십시오

- "Astra Control API를 사용합니다"

스토리지 백엔드를 관리합니다

Astra Control에서 스토리지 클러스터를 스토리지 백엔드로 관리하면 PVS(영구적 볼륨)와 스토리지 백엔드 간의 연결 및 추가 스토리지 메트릭을 얻을 수 있습니다. Astra Control Center가 Cloud Insights에 연결된 경우, 스토리지 용량과 상태 세부 정보를 모니터링할 수 있습니다.

Astra Control API를 사용하여 스토리지 백엔드를 관리하는 방법에 대한 지침은 를 참조하십시오 "Astra 자동화 및 API 정보".

스토리지 백엔드 관리와 관련된 다음 작업을 완료할 수 있습니다.

- "스토리지 백엔드를 추가합니다"
- 스토리지 백엔드 세부 정보를 봅니다
- 스토리지 백엔드의 관리를 취소합니다

- Astra Data Store 스토리지 백엔드 라이센스를 업데이트합니다
- Astra Data Store 스토리지 백엔드를 업그레이드합니다
- 스토리지 백엔드를 제거합니다
- 스토리지 백엔드 클러스터에 노드를 추가합니다
- 스토리지 백엔드 클러스터에서 노드를 제거합니다

스토리지 백엔드 세부 정보를 봅니다

Dashboard 또는 Backend 옵션에서 스토리지 백엔드 정보를 볼 수 있습니다.

스토리지 백엔드 세부 정보 페이지의 Astra Data Store에서 다음 정보를 확인할 수 있습니다.

- Astra Data Store 클러스터
  - 처리량, IOPS, 지연 시간
  - 사용된 용량과 총 용량 비교
- 각 Astra Data Store 클러스터 볼륨에 대해
  - 사용된 용량과 총 용량 비교
  - 처리량

대시보드에서 스토리지 백엔드 세부 정보를 봅니다

단계

1. 왼쪽 탐색 모음에서 * 대시보드 * 를 선택합니다.
2. 상태를 보여 주는 스토리지 백엔드 섹션을 검토합니다.
   - * 비정상 *: 스토리지가 최적 상태가 아닙니다. 이는 지연 시간 문제 또는 컨테이너 문제로 인해 앱 성능이 저하되었기 때문일 수 있습니다.
   - * 모두 정상 *: 스토리지가 관리되었으며 최적의 상태입니다.
   - * 검색됨 *: 스토리지를 검색했지만 Astra Control에서 관리하지 않았습니다.

백엔드 옵션에서 스토리지 백엔드 세부 정보를 봅니다

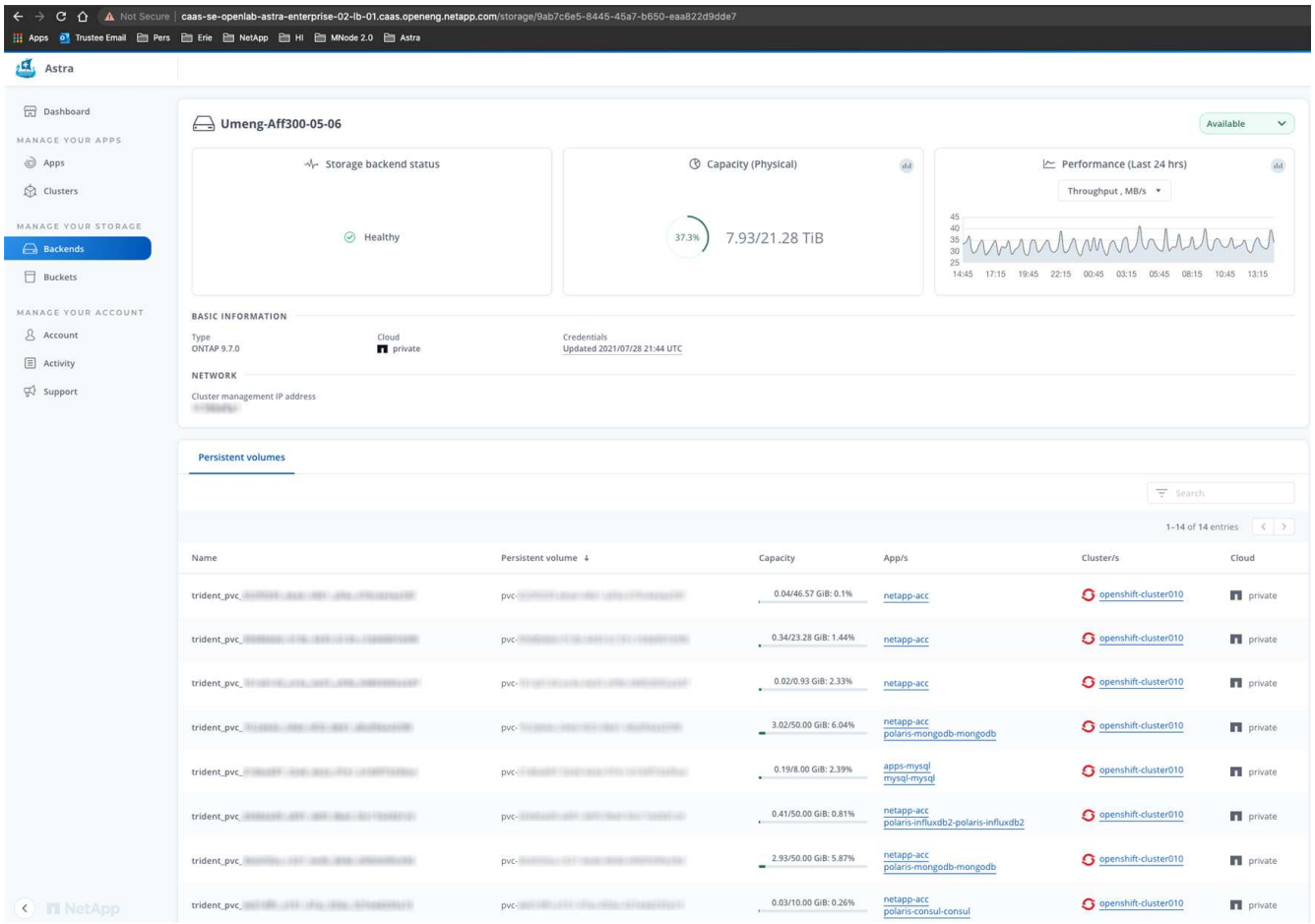
백엔드 상태, 용량 및 성능(IOPS 처리량 및/또는 지연 시간)에 대한 정보를 봅니다.

Kubernetes 앱이 사용 중인 볼륨을 볼 수 있습니다. 볼륨은 선택한 스토리지 백엔드에 저장됩니다. Cloud Insights를 사용하면 추가 정보를 볼 수 있습니다. 을 참조하십시오 "Cloud Insights 설명서".

단계

1. 왼쪽 탐색 영역에서 * backends * 를 선택합니다.
2. 스토리지 백엔드를 선택합니다.

> NetApp Cloud Insights에 연결한 경우 Cloud Insights에서 발췌한 데이터가 백엔드 페이지에 나타납니다.



3. Cloud Insights로 바로 이동하려면 메트릭 이미지 옆에 있는 * Cloud Insights * 아이콘을 선택합니다.

스토리지 백엔드의 관리를 취소합니다

백엔드의 관리를 해제할 수 있습니다.

단계

1. 왼쪽 탐색에서 * backends * 를 선택합니다.
2. 스토리지 백엔드를 선택합니다.
3. Actions * 열의 Options 메뉴에서 * Unmanage * 를 선택합니다.
4. "unmanage"를 입력하여 작업을 확인합니다.
5. Yes, unmanage storage backend * 를 선택합니다.

스토리지 백엔드를 제거합니다

더 이상 사용되지 않는 스토리지 백엔드를 제거할 수 있습니다. 구성을 간단하고 최신 상태로 유지하기 위해 이 작업을 수행할 수 있습니다.

> Astra Data Store 백엔드를 제거하는 경우 vCenter에서 이를 생성하지 않아야 합니다.

필요한 것

- 스토리지 백엔드가 관리되지 않는 상태인지 확인합니다.
- 스토리지 백엔드에 Astra Data Store 클러스터와 연결된 볼륨이 없는지 확인합니다.

단계

1. 왼쪽 탐색에서 * backends * 를 선택합니다.
2. 백엔드가 관리되는 경우 관리를 해제합니다.
   a. Managed * 를 선택합니다.
   b. 스토리지 백엔드를 선택합니다.
   c. Actions * 옵션에서 * Unmanage * 를 선택합니다.
   d. "unmanage"를 입력하여 작업을 확인합니다.
   e. Yes, unmanage storage backend * 를 선택합니다.
3. 검색된 * 를 선택합니다.
   a. 스토리지 백엔드를 선택합니다.
   b. Actions * 옵션에서 * Remove * 를 선택합니다.
   c. 작업을 확인하려면 "remove"를 입력합니다.
   d. Yes, remove storage backend * 를 선택합니다.

Astra Data Store 스토리지 백엔드 라이센스를 업데이트합니다

Astra Data Store 스토리지 백엔드에 대한 라이센스를 업데이트하여 더 큰 구축 또는 향상된 기능을 지원할 수 있습니다.

필요한 것

- 구축 및 관리되는 Astra Data Store 스토리지 백엔드
- Astra Data Store 라이센스 파일(Astra Data Store 라이센스 구매 시 NetApp 세일즈 담당자에게 문의)

단계

1. 왼쪽 탐색에서 * backends * 를 선택합니다.
2. 스토리지 백엔드의 이름을 선택합니다.
3. 기본 정보 * 에서 설치된 라이센스 유형을 확인할 수 있습니다.

   라이센스 정보 위로 마우스를 가져가면 만료 및 권한 정보와 같은 추가 정보가 포함된 팝업이 나타납니다.

4. 라이센스 * 에서 라이센스 이름 옆에 있는 편집 아이콘을 선택합니다.
5. 라이센스 업데이트 * 페이지에서 다음 중 하나를 수행합니다.

라이센스 상태입니다	조치
Astra Data Store에 하나 이상의 라이센스가 추가되었습니다.	목록에서 라이센스를 선택합니다.

라이센스 상태입니다	조치
Astra Data Store에 추가된 라이센스가 없습니다.	a. 추가 * 버튼을 선택합니다. b. 업로드할 라이센스 파일을 선택합니다. c. 라이센스 파일을 업로드하려면 * 추가 * 를 선택하십시오.

6. Update * 를 선택합니다.

Astra Data Store 스토리지 백엔드를 업그레이드합니다

Astra Control Center 내에서 Astra Data Store 백엔드를 업그레이드할 수 있습니다. 이렇게 하려면 먼저 업그레이드 패키지를 업로드해야 합니다. Astra Control Center는 이 업그레이드 패키지를 사용하여 Astra Data Store를 업그레이드합니다.

필요한 것

- 관리 Astra Data Store 스토리지 백엔드
- 업로드된 Astra Data Store 업그레이드 패키지(참조 "소프트웨어 패키지를 관리합니다")

단계

1. backends * 를 선택합니다.
2. 목록에서 Astra Data Store 스토리지 백엔드를 선택하고 * Actions * 열에서 해당 메뉴를 선택합니다.
3. 업그레이드 * 를 선택합니다.
4. 목록에서 업그레이드 버전을 선택합니다.

   리포지토리에 다른 버전의 여러 업그레이드 패키지가 있는 경우 드롭다운 목록을 열어 필요한 버전을 선택할 수 있습니다.

5. 다음 * 을 선택합니다.
6. 업그레이드 시작 * 을 선택합니다.

결과

업그레이드가 완료될 때까지 * backends * 페이지에 * Status * 열에 * Upgrading * 상태가 표시됩니다.

스토리지 백엔드 클러스터에 노드를 추가합니다

Astra Data Store 클러스터에 노드를 추가할 수 있으며, Astra Data Store에 설치된 라이센스 유형으로 지원되는 노드 수까지 추가할 수 있습니다.

필요한 것

- 구축 및 라이센스가 부여된 Astra Data Store 스토리지 백엔드
- Astra Control Center에 Astra Data Store 소프트웨어 패키지를 추가했습니다
- 클러스터에 추가할 새 노드 하나 이상

단계

1. 왼쪽 탐색에서 * backends * 를 선택합니다.
2. 스토리지 백엔드의 이름을 선택합니다.
3. 기본 정보 아래에서 이 스토리지 백엔드 클러스터의 노드 수를 확인할 수 있습니다.
4. 노드 * 에서 노드 수 옆에 있는 편집 아이콘을 선택합니다.
5. 노드 추가 * 페이지에서 새 노드에 대한 정보를 입력합니다.
   a. 각 노드에 대해 노드 레이블을 할당합니다.
   b. 다음 중 하나를 수행합니다.
      - Astra Data Store가 항상 라이센스에 따라 사용 가능한 최대 노드 수를 사용하도록 하려면 * 항상 허용된 최대 노드 수 사용 * 확인란을 활성화합니다.
      - Astra Data Store에서 항상 최대 사용 가능한 노드 수를 사용하지 않으려면 원하는 총 노드 수를 선택합니다.
   c. Protection Domains가 설정된 상태에서 Astra Data Store를 구축한 경우 새 노드를 보호 도메인에 할당합니다.
6. 다음 * 을 선택합니다.
7. 각 새 노드에 대한 IP 주소 및 네트워크 정보를 입력합니다. 단일 새 노드의 단일 IP 주소 또는 여러 새 노드의 IP 주소 풀을 입력합니다.

   Astra Data Store가 구축 중에 구성된 IP 주소를 사용할 수 있는 경우 IP 주소 정보를 입력할 필요가 없습니다.
8. 다음 * 을 선택합니다.
9. 새 노드에 대한 구성을 검토합니다.
10. 노드 추가 * 를 선택합니다.

스토리지 백엔드 클러스터에서 노드를 제거합니다

Astra Data Store 클러스터에서 노드를 제거할 수 있습니다. 이러한 노드는 정상 또는 장애가 발생한 노드일 수 있습니다.

Astra Data Store 클러스터에서 노드를 제거하면 해당 데이터가 클러스터의 다른 노드로 이동하고 Astra Data Store에서 노드가 제거됩니다.

이 프로세스에는 다음 조건이 필요합니다.

- 다른 노드에 데이터를 수신할 수 있는 충분한 여유 공간이 있어야 합니다.
- 클러스터에 4개 이상의 노드가 있어야 합니다.

단계

1. 왼쪽 탐색에서 * backends * 를 선택합니다.
2. 스토리지 백엔드의 이름을 선택합니다.
3. 노드 * 탭을 선택합니다.
4. 작업 메뉴에서 * 제거 * 를 선택합니다.
5. "remove"를 입력하여 삭제를 확인합니다.

6. 예, 노드 제거 * 를 선택합니다.

자세한 내용을 확인하십시오

- "Astra Control API를 사용합니다"

Cloud Insights 및 Fluentd 연결을 통해 인프라를 모니터링합니다

Astra Control Center 환경을 향상시키기 위해 몇 가지 선택적 설정을 구성할 수 있습니다. 전체 인프라를 모니터링하고 통찰력을 확보하기 위해 NetApp Cloud Insights에 연결합니다. Astra Control Center에서 모니터링하는 시스템에서 Kubernetes 이벤트를 수집하려면 Fluentd 연결을 추가합니다.

Astra Control Center를 실행 중인 네트워크에 인터넷에 연결하기 위한 프록시가 필요한 경우(지원 번들을 NetApp Support 사이트에 업로드하거나 Cloud Insights에 연결하려면) Astra Control Center에서 프록시 서버를 구성해야 합니다.

Astra Control Center 스토리지 백엔드 페이지에서 Astra Data Store 스토리지 백엔드 처리량, IOPS 및 용량을 모니터링할 수도 있습니다. 을 참조하십시오 "스토리지 백엔드 관리".

Cloud Insight 또는 NetApp Support 사이트에 연결하기 위한 프록시 서버를 추가합니다

Astra Control Center를 실행 중인 네트워크에 인터넷에 연결하기 위한 프록시가 필요한 경우(지원 번들을 NetApp Support 사이트에 업로드하거나 Cloud Insights에 연결하려면) Astra Control Center에서 프록시 서버를 구성해야 합니다.

> Astra Control Center는 프록시 서버에 대해 입력한 세부 정보를 확인하지 않습니다. 올바른 값을 입력했는지 확인하십시오.

단계

1. admin * / * owner * 권한이 있는 계정을 사용하여 Astra Control Center에 로그인합니다.
2. 계정 * > * 연결 * 을 선택합니다.
3. 드롭다운 목록에서 * 연결 * 을 선택하여 프록시 서버를 추가합니다.

4. 프록시 서버 이름 또는 IP 주소와 프록시 포트 번호를 입력합니다.
5. 프록시 서버에 인증이 필요한 경우 확인란을 선택하고 사용자 이름과 암호를 입력합니다.
6. Connect * 를 선택합니다.

결과

입력한 프록시 정보가 저장된 경우 * 계정 * > * 연결 * 페이지의 * HTTP 프록시 * 섹션에서 해당 정보가 연결되었음을 나타내고 서버 이름을 표시합니다.

프록시 서버 설정을 편집합니다

프록시 서버 설정을 편집할 수 있습니다.

단계

1. admin * / * owner * 권한이 있는 계정을 사용하여 Astra Control Center에 로그인합니다.
2. 계정 * > * 연결 * 을 선택합니다.
3. 드롭다운 목록에서 * 편집 * 을 선택하여 연결을 편집합니다.
4. 서버 세부 정보 및 인증 정보를 편집합니다.
5. 저장 * 을 선택합니다.

프록시 서버 연결을 비활성화합니다

프록시 서버 연결을 비활성화할 수 있습니다. 다른 연결이 중단될 수 있다는 것을 비활성화하기 전에 경고가 표시됩니다.

단계

1. admin * / * owner * 권한이 있는 계정을 사용하여 Astra Control Center에 로그인합니다.
2. 계정 * > * 연결 * 을 선택합니다.
3. 드롭다운 목록에서 * 연결 끊기 * 를 선택하여 연결을 비활성화합니다.
4. 대화 상자가 열리면 작업을 확인합니다.

Cloud Insights에 연결합니다

전체 인프라를 모니터링하고 통찰력을 확보하기 위해 NetApp Cloud Insights을 Astra Control Center 인스턴스와 연결합니다. Cloud Insights는 Astra Control Center 라이선스에 포함되어 있습니다.

Cloud Insights는 Astra Control Center가 사용하는 네트워크나 프록시 서버를 통해 간접적으로 액세스할 수 있어야 합니다.

Astra Control Center가 Cloud Insights에 연결되면 획득 장치 포드가 생성됩니다. 이 Pod는 Astra Control Center에서 관리하는 스토리지 백엔드에서 데이터를 수집하여 Cloud Insights로 푸시합니다. 이 POD에는 8GB RAM과 2개의 CPU 코어가 필요합니다.

또한 Astra Control(Cloud Insights에 연결된)에서 Astra Data Store 클러스터를 관리하는 경우 Astra Data Store 클러스터마다 Astra Data Store에 획득 유닛 포드가 생성되고 Astra Data Store에서 페어링된 Cloud Insights 시스템으로 메트릭이 전송됩니다. 각 Pod에는 8GB RAM과 2개의 CPU 코어가 필요합니다.

Cloud Insights 연결을 설정한 후에는 * backends * 페이지에서 처리량 정보를 확인하고 스토리지 백엔드를 선택한 후 여기에서 Cloud Insights에 연결할 수 있습니다. 또한 클러스터 섹션의 * 대시보드 * 에서 정보를 찾고 Cloud Insights에 연결할 수도 있습니다.

필요한 것

- Astra Control Center 계정에는 * admin * / * owner * 권한이 있습니다.
- 유효한 Astra Control Center 라이센스가 있습니다.
- Astra Control Center를 실행 중인 네트워크에 인터넷에 연결하기 위한 프록시가 필요한 경우 프록시 서버

Cloud Insights를 처음 사용하는 경우 기능과 특징을 잘 익히십시오. 을 참조하십시오 "Cloud Insights 설명서".

단계

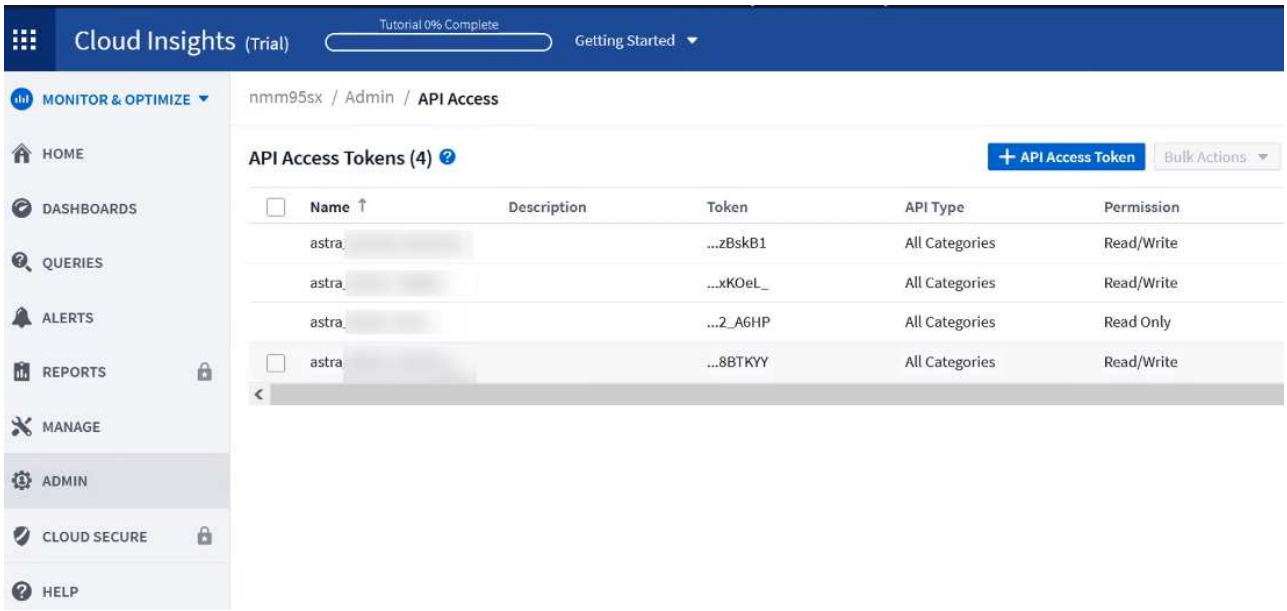
1. admin * / * owner * 권한이 있는 계정을 사용하여 Astra Control Center에 로그인합니다.
2. 계정 * > * 연결 * 을 선택합니다.
3. 연결을 추가하려면 드롭다운 목록에서 * 연결 끊김 * 이 표시되는 * 연결 * 을 선택합니다.

4. Cloud Insights API 토큰 및 테넌트 URL을 입력합니다. 테넌트 URL의 형식은 다음과 같습니다.

```
https://<environment-name>.c01.cloudinsights.netapp.com/
```

Cloud Insights 라이센스가 있으면 테넌트 URL을 가져옵니다. 테넌트 URL이 없는 경우 을 참조하십시오 "Cloud Insights 설명서".

a. 를 다운로드하십시오 "API 토큰"에서 Cloud Insights 테넌트 URL에 로그인합니다.
b. Cloud Insights에서 * 관리자 * > * API 액세스 * 를 클릭하여 * 읽기/쓰기 * 와 * 읽기 전용 * API 액세스 토큰을 모두 생성합니다.



c. 읽기 전용 * 키를 복사합니다. Cloud Insights 연결을 활성화하려면 Astra Control Center 창에 붙여 넣어야 합니다. Read API Access Token 키 권한에 대해 Assets, Alerts, Acquisition Unit 및 Data Collection을 선택합니다.

d. 읽기/쓰기 * 키를 복사합니다. Astra Control Center * Connect Cloud Insights * 창에 붙여 넣어야 합니다. 읽기/쓰기 API 액세스 토큰 키 권한에 대해 자산, 데이터 수집, 로그 수집, 획득 단위, 및 데이터 수집 을 참조하십시오.

> 읽기 전용 * 키와 * 읽기/쓰기 * 키를 생성하고 두 가지 용도로 동일한 키를 사용하지 않는 것이 좋습니다. 기본적으로 토큰 만료 기간은 1년으로 설정됩니다. 토큰이 만료되기 전에 토큰을 최대 지속 시간으로 지정할 수 있도록 기본 선택을 유지하는 것이 좋습니다. 토큰이 만료되면 원격 측정이 중지됩니다.

e. Cloud Insights에서 복사한 키를 Astra Control Center에 붙여 넣습니다.

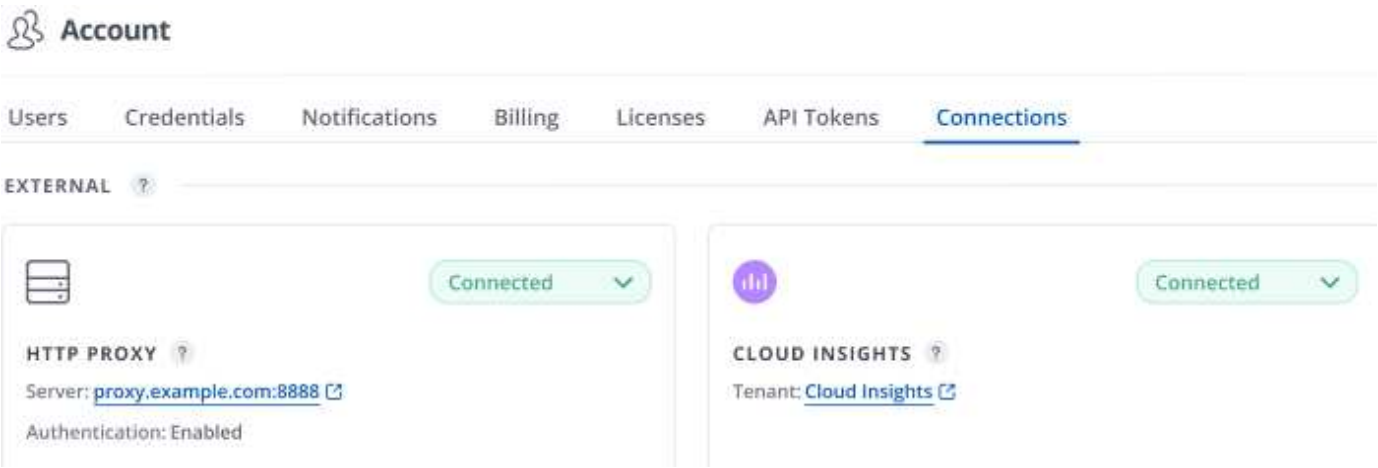
5. Connect * 를 선택합니다.

> 연결을 선택하면 * 연결 상태가 * 계정 * > * 연결 * 페이지의 * Cloud Insights * 섹션에서 * 보류 * 로 변경됩니다. 연결이 활성화되고 상태가 * 연결됨 * 으로 변경되는 데 몇 분 정도 걸릴 수 있습니다.

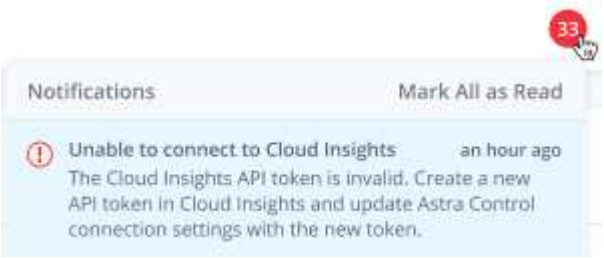
> Astra Control Center와 Cloud Insights UI 사이를 쉽게 오갈 수 있도록 두 가지 모두에 로그인했는지 확인하십시오.

Cloud Insights에서 데이터를 봅니다

연결에 성공하면 * 계정 * > * 연결 * 페이지의 * Cloud Insights * 섹션에 연결된 것으로 표시되고 테넌트 URL이 표시됩니다. Cloud Insights를 방문하여 성공적으로 수신 및 표시된 데이터를 볼 수 있습니다.

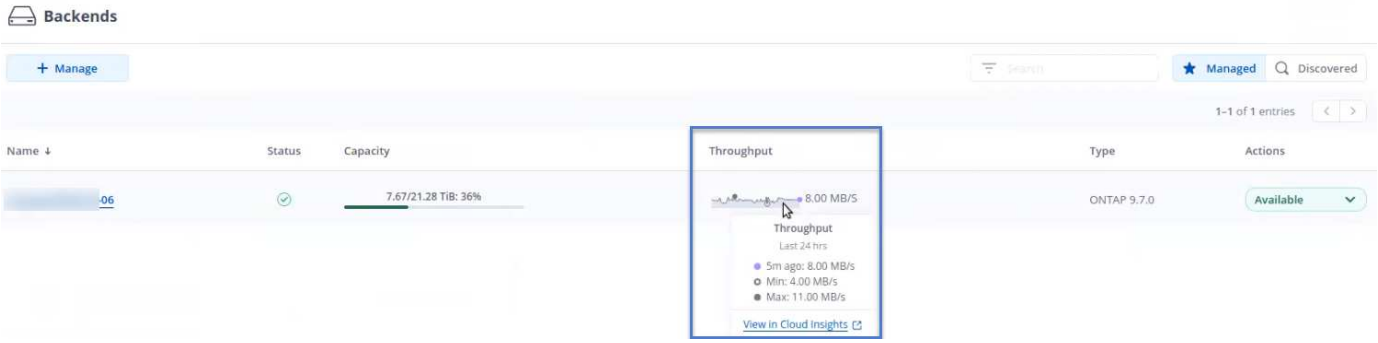


어떤 이유로 연결에 실패한 경우 상태가 * 실패 * 로 표시됩니다. UI 오른쪽 상단의 * 알림 * 에서 실패 원인을 찾을 수 있습니다.



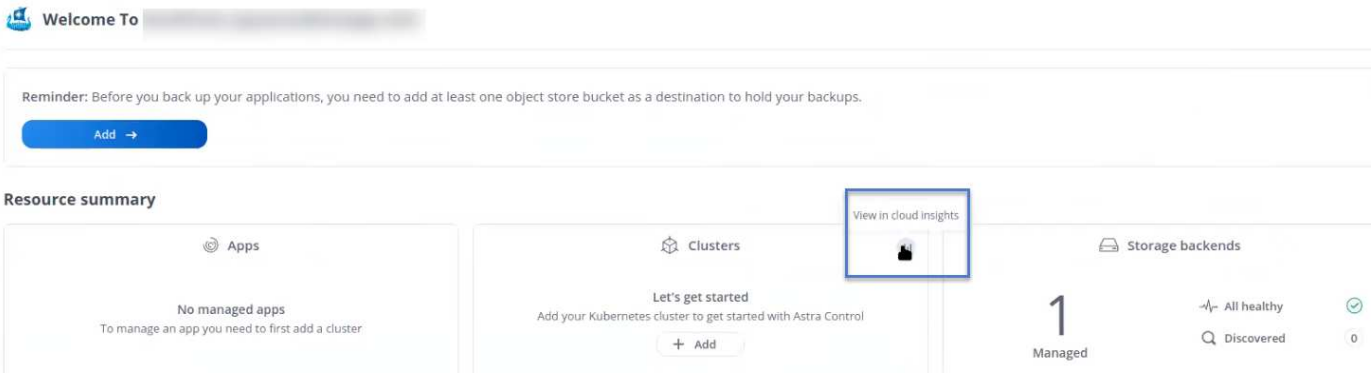
계정 * > * 알림 * 에서 동일한 정보를 찾을 수도 있습니다.

Astra Control Center에서 * backend * 페이지의 처리량 정보를 볼 수 있을 뿐 아니라 스토리지 백엔드를 선택한 후 여기에서 Cloud Insights에 연결할 수도 있습니다
.



Cloud Insights로 바로 이동하려면 메트릭 이미지 옆에 있는 * Cloud Insights * 아이콘을 선택합니다.

또한 * 대시보드 * 에서 정보를 찾을 수 있습니다.



> Cloud Insights 연결을 활성화한 후 Astra 제어 센터에서 추가한 백엔드를 제거하면 백엔드에서 Cloud Insights에 대한 보고를 중지합니다.

Cloud Insights 연결을 편집합니다

Cloud Insights 연결을 편집할 수 있습니다.

> API 키만 편집할 수 있습니다. Cloud Insights 테넌트 URL을 변경하려면 Cloud Insights 연결을 끊고 새 URL에 연결하는 것이 좋습니다.

단계

1. admin * / * owner * 권한이 있는 계정을 사용하여 Astra Control Center에 로그인합니다.
2. 계정 * > * 연결 * 을 선택합니다.
3. 드롭다운 목록에서 * 편집 * 을 선택하여 연결을 편집합니다.
4. Cloud Insights 연결 설정을 편집합니다.
5. 저장 * 을 선택합니다.

Cloud Insights 연결을 비활성화합니다

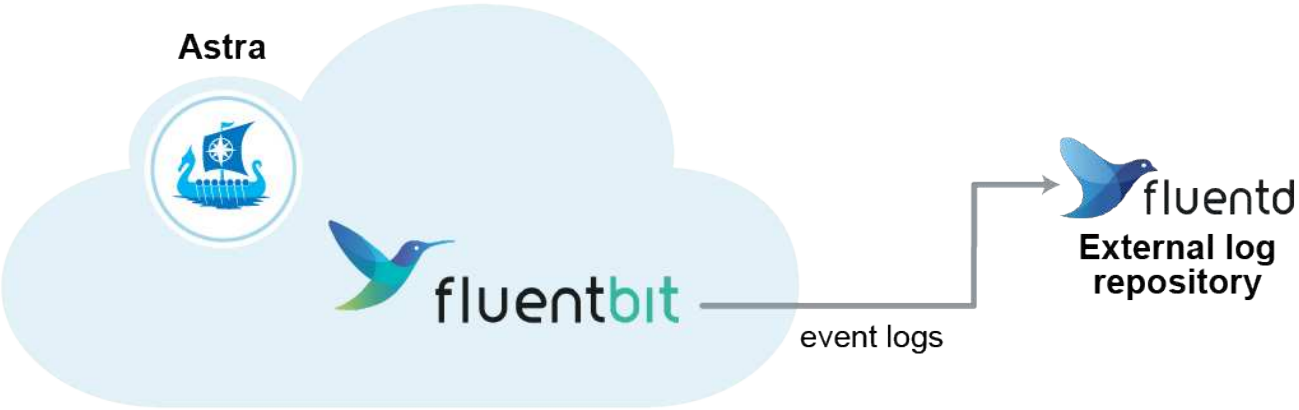
Astra Control Center에서 관리하는 Kubernetes 클러스터에 대한 Cloud Insights 연결을 해제할 수 있습니다. Cloud Insights 연결을 비활성화해도 이미 Cloud Insights에 업로드된 원격 측정 데이터는 삭제되지 않습니다.

단계

1. admin * / * owner * 권한이 있는 계정을 사용하여 Astra Control Center에 로그인합니다.
2. 계정 * > * 연결 * 을 선택합니다.
3. 드롭다운 목록에서 * 연결 끊기 * 를 선택하여 연결을 비활성화합니다.
4. 대화 상자가 열리면 작업을 확인합니다. 작업을 확인한 후 * 계정 * > * 연결 * 페이지에서 Cloud Insights 상태가 * 보류 * 로 변경됩니다. 상태가 * 연결 끊김 * 으로 변경되는 데 몇 분 정도 걸립니다.

Fluentd에 연결합니다

Astra Control Center에서 Fluentd 엔드포인트로 로그(Kubernetes 이벤트)를 보낼 수 있습니다. Fluentd 연결은 기본적으로 비활성화되어 있습니다.



관리되는 클러스터의 이벤트 로그만 Fluentd로 전달됩니다.

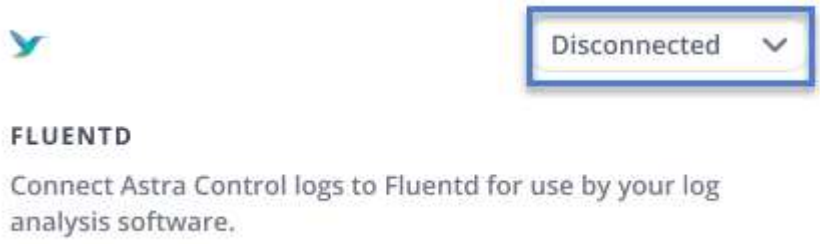
필요한 것

- Astra Control Center 계정에는 * admin * / * owner * 권한이 있습니다.
- Kubernetes 클러스터에 설치 및 실행 중인 Astra Control Center

Astra Control Center는 Fluentd 서버에 대해 입력한 세부 정보를 확인하지 않습니다. 올바른 값을 입력했는지 확인하십시오.

단계

1. admin * / * owner * 권한이 있는 계정을 사용하여 Astra Control Center에 로그인합니다.
2. 계정 * > * 연결 * 을 선택합니다.
3. 연결을 추가하려면 * 연결 끊김 * 이 표시된 드롭다운 목록에서 * 연결 * 을 선택합니다.



4. Fluentd 서버의 호스트 IP 주소, 포트 번호 및 공유 키를 입력합니다.
5. Connect * 를 선택합니다.

결과

Fluentd 서버에 대해 입력한 세부 정보가 저장된 경우 * 계정 * > * 연결 * 페이지의 * Fluentd * 섹션에서 해당 정보가 연결되었음을 나타냅니다. 이제 연결한 Fluentd 서버를 방문하여 이벤트 로그를 볼 수 있습니다.

어떤 이유로 연결에 실패한 경우 상태가 * 실패 * 로 표시됩니다. UI 오른쪽 상단의 * 알림 * 에서 실패 원인을 찾을 수 있습니다.

계정 * > * 알림 * 에서 동일한 정보를 찾을 수도 있습니다.

로그 수집에 문제가 있는 경우 작업자 노드에 로그인하여 에서 로그를 사용할 수 있는지 확인해야 합니다 `/var/log/containers/`.

Fluentd 연결을 편집합니다

Fluentd 연결을 Astra Control Center 인스턴스에 편집할 수 있습니다.

단계

1. admin * / * owner * 권한이 있는 계정을 사용하여 Astra Control Center에 로그인합니다.
2. 계정 * > * 연결 * 을 선택합니다.
3. 드롭다운 목록에서 * 편집 * 을 선택하여 연결을 편집합니다.
4. Fluentd 끝점 설정을 변경합니다.
5. 저장 * 을 선택합니다.

Fluentd 연결을 비활성화합니다

Astra Control Center 인스턴스에 대한 Fluentd 연결을 비활성화할 수 있습니다.

단계

1. admin * / * owner * 권한이 있는 계정을 사용하여 Astra Control Center에 로그인합니다.
2. 계정 * > * 연결 * 을 선택합니다.
3. 드롭다운 목록에서 * 연결 끊기 * 를 선택하여 연결을 비활성화합니다.
4. 대화 상자가 열리면 작업을 확인합니다.

앱 및 클러스터 관리를 취소합니다

Astra Control Center에서 더 이상 관리하지 않으려는 응용 프로그램 또는 클러스터를 제거합니다.

앱 관리를 취소합니다

Astra Control Center에서 더 이상 백업, 스냅샷 또는 클론 복제하지 않을 애플리케이션 관리를 중지합니다.

- 기존 백업 및 스냅샷이 삭제됩니다.
- 애플리케이션과 데이터는 사용 가능한 상태로 유지됩니다.

단계

1. 왼쪽 탐색 모음에서 * 응용 프로그램 * 을 선택합니다.
2. 더 이상 관리하지 않을 앱의 확인란을 선택합니다.
3. Action * 메뉴에서 * Unmanage * 를 선택합니다.
4. "unmanage"를 입력하여 확인합니다.
5. 앱 관리를 해제할지 확인한 다음 * 예, 애플리케이션 관리 취소 * 를 선택합니다.

결과

Astra Control Center가 앱 관리를 중지합니다.

클러스터 관리를 취소합니다

Astra Control Center에서 더 이상 관리하지 않으려는 클러스터를 관리 해제합니다.

- 이 작업을 수행하면 Astra Control Center에서 클러스터를 관리할 수 없습니다. 클러스터 구성을 변경하지 않고 클러스터를 삭제하지 않습니다.
- Trident가 클러스터에서 제거되지 않습니다. "Trident를 제거하는 방법을 알아보십시오".

> 클러스터를 관리하기 전에 클러스터와 연결된 앱의 관리를 해제해야 합니다.

단계

1. 왼쪽 탐색 모음에서 * 클러스터 * 를 선택합니다.
2. Astra Control Center에서 더 이상 관리하지 않으려는 클러스터의 확인란을 선택합니다.
3. Actions * 열의 Options 메뉴에서 * Unmanage * 를 선택합니다.
4. 클러스터 관리를 해제할지 확인한 다음 * 예, 클러스터 관리 취소 * 를 선택합니다.

결과

클러스터의 상태가 * Removing * 으로 변경되고 그 후에는 * Clusters * 페이지에서 클러스터가 제거되고 Astra Control Center에서 더 이상 관리되지 않습니다.

> * Astra Control Center와 Cloud Insights가 연결되지 않은 경우 * 클러스터를 관리하지 않으면 원격 측정 데이터를 전송하기 위해 설치된 모든 리소스가 제거됩니다. * Astra Control Center와 Cloud Insights가 연결된 경우 * 클러스터를 관리하지 않으면 만 삭제됩니다 `fluentbit` 및 `event-exporter` Pod를 클릭합니다.

Astra Control Center를 업그레이드합니다

Astra Control Center를 업그레이드하려면 NetApp Support 사이트에서 설치 번들을 다운로드하고 해당 지침에 따라 Astra Control Center 구성 요소를 업그레이드하십시오. 이 절차를 사용하여 인터넷에 연결되거나 공기가 연결된 환경에서 Astra Control Center를 업그레이드할 수 있습니다.

필요한 것

- "업그레이드를 시작하기 전에 운영 환경이 Astra Control Center 배포에 대한 최소 요구 사항을 충족하는지 확인하십시오".
- 모든 클러스터 운영자가 양호한 상태이며 사용 가능한지 확인합니다.

```
kubectl get clusteroperators
```

- 모든 API 서비스가 정상 상태이며 사용 가능한지 확인합니다.

```
kubectl get apiservices
```

- Astra Control Center에서 로그아웃합니다.

이 작업에 대해

Astra Control Center 업그레이드 프로세스는 다음과 같은 고급 단계를 안내합니다.

- Astra Control Center 번들을 다운로드합니다
- 번들의 포장을 풀고 디렉토리를 변경합니다
- 이미지를 로컬 레지스트리에 추가합니다
- 업데이트된 Astra Control Center 운영자를 설치합니다
- Astra Control Center를 업그레이드합니다
- 타사 서비스 업그레이드(선택 사항)
- 시스템 상태를 확인합니다
- 부하 분산을 위한 수신 설정

모든 Astra Control Center Pod를 삭제하지 않도록 전체 업그레이드 프로세스 중에 다음 명령을 실행하지 마십시오. `kubectl delete -f astra_control_center_operator_deploy.yaml`

스케줄, 백업 및 스냅샷이 실행되고 있지 않은 경우 유지보수 창에서 업그레이드를 수행합니다.

Docker Engine 대신 Red Hat의 Podman 명령을 사용하는 경우 Docker 명령 대신 Podman 명령을 사용할 수 있습니다.

Astra Control Center 번들을 다운로드합니다

1. Astra Control Center 업그레이드 번들을 다운로드합니다 (`astra-control-center-[version].tar.gz`) https: mysupport.netapp.com/site/products/all/details/astra-control-center/downloads-tab[NetApp 지원 사이트^]에서.
2. (선택 사항) 다음 명령을 사용하여 번들의 서명을 확인합니다.

```
openssl dgst -sha256 -verify AstraControlCenter-public.pub -signature
astra-control-center-[version].tar.gz.sig astra-control-center-
[version].tar.gz
```

번들의 포장을 풀고 디렉토리를 변경합니다

1. 이미지 추출:

```
tar -vxzf astra-control-center-[version].tar.gz
```

이미지를 로컬 레지스트리에 추가합니다

1. 용기 엔진에 적합한 단계 시퀀스를 완료합니다.

Docker 를 참조하십시오

1. Astra 디렉토리로 이동합니다.

```
cd acc
```

2. Astra Control Center 이미지 디렉토리에 있는 패키지 이미지를 로컬 레지스트리로 푸시합니다. 명령을 실행하기 전에 다음 대체 작업을 수행합니다.
   - Bundle_file을 Astra Control 번들 파일 이름으로 바꿉니다(예: `acc.manifest.yaml`)를 클릭합니다.
   - my_registry를 Docker 리포지토리의 URL로 바꿉니다.
   - my_registry_user를 사용자 이름으로 바꿉니다.
   - my_registry_token을 레지스트리에 대한 인증된 토큰으로 바꿉니다.

```
kubectl astra packages push-images -m BUNDLE_FILE -r MY_REGISTRY
-u MY_REGISTRY_USER -p MY_REGISTRY_TOKEN
```

팟맨

1. 레지스트리에 로그인합니다.

```
podman login [your_registry_path]
```

2. 설명에 명시된 대로 <your_registry> 대체를 만들어 다음 스크립트를 실행합니다.

```
# You need to be at the root of the tarball.
# You should see these files to confirm correct location:
#   acc.manifest.yaml
#   acc/

# Replace <YOUR_REGISTRY> with your own registry (e.g
registry.customer.com or registry.customer.com/testing, etc..)
export REGISTRY=<YOUR_REGISTRY>
export PACKAGENAME=acc
export PACKAGEVERSION=22.08.1-26
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
  # Load to local cache
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')

  # Remove path and keep imageName.
  astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')

  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/netapp/astra/${PACKAGENAME}
/${PACKAGEVERSION}/${astraImageNoPath}

  # Push to the local repo.
  podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done
```

업데이트된 **Astra Control Center** 운영자를 설치합니다

1. 디렉토리를 변경합니다.

```
cd manifests
```

2. Astra Control Center 운영자 배포 YAML을 편집합니다 (`astra_control_center_operator_deploy.yaml`)를 클릭하여 로컬 레지스트리 및 암호를 참조합니다.

```
vim astra_control_center_operator_deploy.yaml
```

   a. 인증이 필요한 레지스트리를 사용하는 경우 의 기본 줄을 바꿉니다 `imagePullSecrets: []` 다음 포함:

```
imagePullSecrets:
- name: <name_of_secret_with_creds_to_local_registry>
```

b. 변경 `[your_registry_path]` 의 경우 `kube-rbac-proxy` 이미지를 에서 푸시한 레지스트리 경로로 이미지 이전 단계.

c. 변경 `[your_registry_path]` 의 경우 `acc-operator-controller-manager` 이미지를 에서 푸시한 레지스트리 경로로 이미지 이전 단계.

d. 에 다음 값을 추가합니다 `env` 섹션:

```
- name: ACCOP_HELM_UPGRADETIMEOUT
  value: 300m
```

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
  name: acc-operator-controller-manager
  namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
      containers:
      - args:
        - --secure-listen-address=0.0.0.0:8443
        - --upstream=http://127.0.0.1:8080/
        - --logtostderr=true
        - --v=10
        image: [your_registry_path]/kube-rbac-proxy:v4.8.0
        name: kube-rbac-proxy
        ports:
        - containerPort: 8443
          name: https
      - args:
        - --health-probe-bind-address=:8081
        - --metrics-bind-address=127.0.0.1:8080
        - --leader-elect
        command:
        - /manager
        env:
        - name: ACCOP_LOG_LEVEL
          value: "2"
        - name: ACCOP_HELM_UPGRADETIMEOUT
          value: 300m
        image: [your_registry_path]/acc-operator:[version x.y.z]
        imagePullPolicy: IfNotPresent
      imagePullSecrets: []
```

3. 업데이트된 Astra Control Center 운영자를 설치합니다.

```
kubectl apply -f astra_control_center_operator_deploy.yaml
```

샘플 반응:

```
namespace/netapp-acc-operator unchanged
customresourcedefinition.apiextensions.k8s.io/astracontrolcenters.astra.
netapp.io configured
role.rbac.authorization.k8s.io/acc-operator-leader-election-role
unchanged
clusterrole.rbac.authorization.k8s.io/acc-operator-manager-role
configured
clusterrole.rbac.authorization.k8s.io/acc-operator-metrics-reader
unchanged
clusterrole.rbac.authorization.k8s.io/acc-operator-proxy-role unchanged
rolebinding.rbac.authorization.k8s.io/acc-operator-leader-election-
rolebinding unchanged
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-manager-
rolebinding configured
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-proxy-
rolebinding unchanged
configmap/acc-operator-manager-config unchanged
service/acc-operator-controller-manager-metrics-service unchanged
deployment.apps/acc-operator-controller-manager configured
```

4. Pod가 실행 중인지 확인합니다.

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

Astra Control Center를 업그레이드합니다

1. Astra Control Center 사용자 지정 리소스(CR) 편집 (`astra_control_center_min.yaml`)를 사용하여 Astra 버전을 변경합니다 (`astraVersion` 의 내부 `Spec`) 번호:

```
kubectl edit acc -n [netapp-acc or custom namespace]
```

> 레지스트리 경로는 에서 이미지를 푸시한 레지스트리 경로와 일치해야 합니다 이전 단계.

2. 에 다음 행을 추가합니다 `additionalValues` 의 내부 `Spec` Astra Control Center CR에서 다음을 수행합니다.

```
additionalValues:
    nautilus:
      startupProbe:
        periodSeconds: 30
        failureThreshold: 600
```

3. 다음 중 하나를 수행합니다.

   a. 자체 IngessController 또는 Ingress가 없고 Traefik 게이트웨이와 함께 Astra Control Center를 로드 밸런서 유형 서비스로 사용하고 있으며 이 설정을 계속하려면 다른 필드를 지정하십시오 `ingressType` (아직 없는 경우) 를 클릭하여 로 설정합니다 `AccTraefik`.

   ```
   ingressType: AccTraefik
   ```

   b. 기본 Astra Control Center 일반 수신 배포로 전환하려면 자체 IngressController/Ingress 설정(TLS 종료 등)을 제공하고 Astra Control Center로 가는 경로를 연 다음 설정합니다 `ingressType` 를 선택합니다 `Generic`.

   ```
   ingressType: Generic
   ```

   필드를 생략하면 프로세스가 일반 배포가 됩니다. 일반 배포를 원하지 않는 경우 필드를 추가해야 합니다.

4. (선택 사항) Pod가 종료되어 다시 사용할 수 있는지 확인합니다.

```
watch kubectl get po -n [netapp-acc or custom namespace]
```

5. Astra 상태 조건이 업그레이드가 완료되어 준비되었음을 나타낼 때까지 기다립니다.

```
kubectl get -o yaml -n [netapp-acc or custom namespace]
astracontrolcenters.astra.netapp.io astra
```

응답:

```
conditions:
  - lastTransitionTime: "2021-10-25T18:49:26Z"
    message: Astra is deployed
    reason: Complete
    status: "True"
    type: Ready
  - lastTransitionTime: "2021-10-25T18:49:26Z"
    message: Upgrading succeeded.
    reason: Complete
    status: "False"
    type: Upgrading
```

6. 다시 로그인하여 관리되는 모든 클러스터와 앱이 여전히 존재하고 보호되고 있는지 확인합니다.
7. 운영자가 Cert-manager를 업데이트하지 않은 경우, 다음으로 타사 서비스를 업그레이드하십시오.

타사 서비스 업그레이드(선택 사항)

타사 서비스 Traefik 및 Cert-manager는 이전 업그레이드 단계 중에 업그레이드되지 않습니다. 여기에 설명된 절차를 사용하여 필요에 따라 업그레이드하거나 시스템에 필요한 경우 기존 서비스 버전을 유지할 수 있습니다.

- * Traefik *: 기본적으로 Astra Control Center는 Traefik 배포의 수명 주기를 관리합니다. 설정 `externalTraefik` 를 선택합니다 `false` (기본값) 시스템에 외부 Traefik이 없고 Astra Control Center에서 Traefik을 설치 및 관리하고 있음을 나타냅니다. 이 경우 `externalTraefik` 가 로 설정되어 있습니다 `false`.

  반면, Traefik 배포가 있는 경우 를 설정합니다 `externalTraefik` 를 선택합니다 `true`. 이 경우 구축을 유지 관리하고 Astra Control Center는 CRD를 업그레이드하지 않습니다 `shouldUpgrade` 가 로 설정되어 있습니다 `true`.

- * Cert-manager *: 기본적으로 Astra Control Center는 사용자가 설정하지 않은 경우 인증서 관리자(및 CRD)를 설치합니다 `externalCertManager` 를 선택합니다 `true`. 설정 `shouldUpgrade` 를 선택합니다 `true` Astra Control Center가 CRD를 업그레이드하도록 합니다.

다음 조건 중 하나라도 충족되면 Traefik이 업그레이드됩니다.

- 외부트래이픽: 거짓
- externalTraefik: true 및 shouldUpgrade: true입니다.

단계

1. 를 편집합니다 `acc` CR:

```
kubectl edit acc -n [netapp-acc or custom namespace]
```

2. 를 변경합니다 `externalTraefik` 필드 및 `shouldUpgrade` 필드를 선택합니다 `true` 또는 `false` 필요 시.

```
crds:
    externalTraefik: false
    externalCertManager: false
    shouldUpgrade: false
```

시스템 상태를 확인합니다

1. Astra Control Center에 로그인합니다.
2. 모든 관리되는 클러스터와 앱이 여전히 존재하고 보호되고 있는지 확인합니다.

부하 분산을 위한 수신 설정

클러스터의 로드 밸런싱과 같은 서비스에 대한 외부 액세스를 관리하는 Kubernetes 수신 객체를 설정할 수 있습니다.

- 기본 업그레이드는 일반적인 수신 배포를 사용합니다. 이 경우 수신 컨트롤러 또는 수신 리소스를 설정해야 합니다.
- 수신 컨트롤러를 원하지 않고 이미 가지고 있는 것을 유지하려면 를 설정합니다 `ingressType` 를 선택합니다 `AccTraefik`.

> "로드 밸런서" 및 수신 서비스 유형에 대한 자세한 내용은 을 참조하십시오 "요구 사항".

단계는 사용하는 수신 컨트롤러의 유형에 따라 다릅니다.

- Nginx 수신 컨트롤러
- OpenShift 수신 컨트롤러

필요한 것

- CR 사양에서
  - If(경우 `crd.externalTraefik` 가 있으면 로 설정해야 합니다 `false` 또는
  - If(경우 `crd.externalTraefik` 있습니다 `true`, `crd.shouldUpgrade` 또한 입니다 `true`.
- 필수 요소입니다 "수신 컨트롤러" 이미 배포되어 있어야 합니다.
- 를 클릭합니다 "수신 클래스" 수신 컨트롤러에 해당하는 컨트롤러가 이미 생성되어야 합니다.
- V1.19 및 v1.21 등의 Kubernetes 버전을 사용하고 있습니다.

Nginx 수신 컨트롤러 단계

1. 기존 암호를 사용합니다 `secure-testing-cert` 또는 형식 암호를 만듭니다[`kubernetes.io/tls`] 에서 TLS 개인 키 및 인증서의 경우 `netapp-acc` 에 설명된 대로 (또는 사용자 지정 이름) 네임스페이스를 사용합니다 "TLS 비밀".
2. 수신 리소스를 에 배포합니다 `netapp-acc` 사용되지 않는 스키마나 새 스키마에 대한 (또는 사용자 지정 이름) 네임스페이스:

   a. 더 이상 사용되지 않는 스키마의 경우 다음 샘플을 따르십시오.

```
apiVersion: extensions/v1beta1
kind: IngressClass
metadata:
  name: ingress-acc
  namespace: [netapp-acc or custom namespace]
  annotations:
    kubernetes.io/ingress.class: nginx
spec:
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: [ACC address]
    http:
      paths:
      - backend:
        serviceName: traefik
        servicePort: 80
        pathType: ImplementationSpecific
```

b. 새 스키마의 경우 다음 예제를 따르십시오.

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: netapp-acc-ingress
  namespace: [netapp-acc or custom namespace]
spec:
  ingressClassName: [class name for nginx controller]
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: <ACC address>
    http:
      paths:
        - path:
          backend:
            service:
              name: traefik
              port:
                number: 80
          pathType: ImplementationSpecific
```

OpenShift Ingress 컨트롤러를 위한 단계

1. 인증서를 구입하고 OpenShift 라우트에서 사용할 수 있도록 준비된 키, 인증서 및 CA 파일을 가져옵니다.
2. OpenShift 경로를 생성합니다.

```
oc create route edge --service=traefik
--port=web -n [netapp-acc or custom namespace]
--insecure-policy=Redirect --hostname=<ACC address>
--cert=cert.pem --key=key.pem
```

수신 설정을 확인합니다

계속하기 전에 수신 설정을 확인할 수 있습니다.

1. Traefik이 (으)로 변경되었는지 확인합니다 `clusterIP` 로드 밸런서:

```
kubectl get service traefik -n [netapp-acc or custom namespace]
```

2. Traefik에서 경로 확인:

```
Kubectl get ingressroute ingressroutetls -n [netapp-acc or custom
namespace]
-o yaml | grep "Host("
```

결과는 비어 있어야 합니다.

Astra Control Center를 제거합니다

평가판을 정식 버전으로 업그레이드하는 경우 Astra Control Center 구성 요소를 제거해야 할 수 있습니다. Astra Control Center 및 Astra Control Center 운영자를 제거하려면 이 절차에 설명된 명령을 순서대로 실행하십시오.

설치 제거에 문제가 있는 경우 를 참조하십시오 제거 문제 해결.

필요한 것

- Astra Control Center UI를 사용하여 모두 관리합니다 "클러스터".

단계

1. Astra Control Center를 삭제합니다. 다음 샘플 명령은 기본 설치를 기반으로 합니다. 사용자 정의 설정을 만든 경우 명령을 수정합니다.

   ```
   kubectl delete -f astra_control_center_min.yaml -n netapp-acc
   ```

   결과:

   ```
   astracontrolcenter.astra.netapp.io "astra" deleted
   ```

2. 다음 명령을 사용하여 를 삭제합니다 `netapp-acc` 네임스페이스:

   ```
   kubectl delete ns netapp-acc
   ```

   결과:

   ```
   namespace "netapp-acc" deleted
   ```

3. 다음 명령을 사용하여 Astra Control Center 운영자 시스템 구성 요소를 삭제합니다.

   ```
   kubectl delete -f astra_control_center_operator_deploy.yaml
   ```

   결과:

```
namespace/netapp-acc-operator deleted
customresourcedefinition.apiextensions.k8s.io/astracontrolcenters.astra.
netapp.io deleted
role.rbac.authorization.k8s.io/acc-operator-leader-election-role deleted
clusterrole.rbac.authorization.k8s.io/acc-operator-manager-role deleted
clusterrole.rbac.authorization.k8s.io/acc-operator-metrics-reader
deleted
clusterrole.rbac.authorization.k8s.io/acc-operator-proxy-role deleted
rolebinding.rbac.authorization.k8s.io/acc-operator-leader-election-
rolebinding deleted
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-manager-
rolebinding deleted
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-proxy-
rolebinding deleted
configmap/acc-operator-manager-config deleted
service/acc-operator-controller-manager-metrics-service deleted
deployment.apps/acc-operator-controller-manager deleted
```

제거 문제 해결

다음 해결 방법을 사용하여 Astra Control Center를 제거할 때 발생하는 문제를 해결하십시오.

Astra Control Center를 제거해도 관리 클러스터의 모니터링 운영자 포드가 정리되지 않습니다

Astra Control Center를 제거하기 전에 클러스터를 관리하지 않았다면 NetApp 모니터링 네임스페이스 및 네임스페이스에서 Pod를 수동으로 삭제할 수 있습니다. 이러한 명령은 다음과 같습니다.

단계

1. 삭제 `acc-monitoring` 에이전트:

   ```
   kubectl delete agents acc-monitoring -n netapp-monitoring
   ```

   결과:

   ```
   agent.monitoring.netapp.com "acc-monitoring" deleted
   ```

2. 네임스페이스 삭제:

   ```
   kubectl delete ns netapp-monitoring
   ```

   결과:

```
namespace "netapp-monitoring" deleted
```

3. 제거된 리소스 확인:

```
kubectl get pods -n netapp-monitoring
```

결과:

```
No resources found in netapp-monitoring namespace.
```

4. 모니터링 에이전트 제거 확인:

```
kubectl get crd|grep agent
```

샘플 결과:

```
agents.monitoring.netapp.com                    2021-07-21T06:08:13Z
```

5. 사용자 정의 리소스 정의(CRD) 정보 삭제:

```
kubectl delete crds agents.monitoring.netapp.com
```

결과:

```
customresourcedefinition.apiextensions.k8s.io
"agents.monitoring.netapp.com" deleted
```

Astra Control Center를 제거해도 **Traefik CRD**가 정리되지 않습니다

Traefik CRD를 수동으로 삭제할 수 있습니다. CRD는 글로벌 리소스이며 CRD를 삭제하면 클러스터의 다른 애플리케이션에 영향을 줄 수 있습니다.

단계

1. 클러스터에 설치된 Traefik CRD 나열:

```
kubectl get crds |grep -E 'traefik'
```

응답

```
ingressroutes.traefik.containo.us             2021-06-23T23:29:11Z
ingressroutetcps.traefik.containo.us          2021-06-23T23:29:11Z
ingressrouteudps.traefik.containo.us          2021-06-23T23:29:12Z
middlewares.traefik.containo.us               2021-06-23T23:29:12Z
middlewaretcps.traefik.containo.us            2021-06-23T23:29:12Z
serverstransports.traefik.containo.us         2021-06-23T23:29:13Z
tlsoptions.traefik.containo.us                2021-06-23T23:29:13Z
tlsstores.traefik.containo.us                 2021-06-23T23:29:14Z
traefikservices.traefik.containo.us           2021-06-23T23:29:15Z
```

2. CRD 삭제:

```
kubectl delete crd ingressroutes.traefik.containo.us
ingressroutetcps.traefik.containo.us
ingressrouteudps.traefik.containo.us middlewares.traefik.containo.us
serverstransports.traefik.containo.us tlsoptions.traefik.containo.us
tlsstores.traefik.containo.us traefikservices.traefik.containo.us
middlewaretcps.traefik.containo.us
```

자세한 내용을 확인하십시오

- "제거 관련 알려진 문제입니다"

REST API를 사용하여 자동화

Astra Control REST API를 사용한 자동화

Astra Control에는 Curl과 같은 프로그래밍 언어나 유틸리티를 사용하여 Astra Control 기능에 직접 액세스할 수 있는 REST API가 있습니다. Ansible 및 기타 자동화 기술을 사용하여 Astra Control 배포를 관리할 수도 있습니다.

Kubernetes 앱을 설정 및 관리하려면 Astra UI 또는 Astra Control API를 사용할 수 있습니다.

자세한 내용은 로 이동하십시오 "Astra 자동화 문서".

지식 및 지원

문제 해결

발생할 수 있는 몇 가지 일반적인 문제를 해결하는 방법에 대해 알아봅니다.

"Astra의 NetApp 기술 자료"

자세한 내용을 확인하십시오

- "NetApp에 파일을 업로드하는 방법(로그인 필요)"
- "파일을 NetApp에 수동으로 업로드하는 방법(로그인 필요)"

도움을 받으십시오

NetApp은 다양한 방법으로 Astra Control을 지원합니다. 기술 자료(KB) 기사 및 불화 채널 같은 광범위한 무료 셀프 지원 옵션이 24x7 제공됩니다. Astra Control 계정에는 웹 발권 서비스를 통한 원격 기술 지원이 포함되어 있습니다.

> Astra Control Center에 대한 평가판 라이센스가 있는 경우 기술 지원을 받을 수 있습니다. 그러나 NSS(NetApp Support Site)를 통한 케이스 생성은 사용할 수 없습니다. 피드백 옵션을 통해 지원을 받거나 불협화음을 셀프 서비스로 사용할 수 있습니다.

먼저 해야 합니다 "NetApp 일련 번호에 대한 지원을 활성화합니다" 이러한 비 셀프 서비스 지원 옵션을 사용하려면 NetApp NSS(Support Site) SSO 계정은 케이스 관리와 함께 채팅 및 웹 티켓팅에 필요합니다.

자체 지원 옵션

기본 메뉴에서 * 지원 * 탭을 선택하면 Astra Control Center UI에서 지원 옵션에 액세스할 수 있습니다.

이러한 옵션은 24x7 무료로 제공됩니다.

- "* 기술 자료 * (로그인 필요)"Astra Control과 관련된 문서, FAQ 또는 고장 수리 정보를 검색합니다.
- * 문서 센터 *: 현재 보고 있는 문서 사이트입니다.
- "* 불화를 통한 도움 받기*": Pub 카테고리의 Astra로 이동하여 동료 및 전문가와 교류하십시오.
- * 지원 케이스 생성 *: 문제 해결을 위해 NetApp 지원에 제공할 지원 번들을 생성합니다.
- * Astra Control에 대한 피드백 제공 *: astra.feedback@netapp.com 으로 이메일을 보내 귀하의 생각, 아이디어 또는 우려 사항을 알려 주십시오.

NetApp Support에 매일 예약된 지원 번들 업로드를 활성화합니다

Astra Control Center를 설치하는 동안(지정된 경우 `enrolled: true` 용 `autoSupport` Astra Control Center 사용자 정의 리소스 정의(CRD) 파일 (`astra_control_center_min.yaml`), 일별 지원 번들은 에 자동으로 업로드됩니다 "NetApp Support 사이트".

NetApp 지원에 제공할 지원 번들을 생성합니다

Astra Control Center를 사용하면 관리자가 NetApp 지원에 유용한 정보, 로그, Astra 구축의 모든 구성 요소에 대한 이벤트, 메트릭, 관리 중인 클러스터와 앱에 대한 토폴로지 정보 등 번들을 생성할 수 있습니다. 인터넷에 연결되어 있는 경우 Astra Control Center UI에서 직접 NSS(NetApp Support Site)에 지원 번들을 업로드할 수 있습니다.

> Astra Control Center에서 번들을 생성하는 데 걸리는 시간은 Astra Control Center 설치 크기와 요청된 지원 번들의 매개 변수에 따라 다릅니다. 지원 번들을 요청할 때 지정한 기간은 번들을 생성하는 데 걸리는 시간을 나타냅니다(예: 기간이 짧을수록 번들 생성 속도가 빠름).

시작하기 전에

NSS에 번들을 업로드하는 데 프록시 연결이 필요한지 여부를 확인합니다. 프록시 연결이 필요한 경우 Astra Control Center가 프록시 서버를 사용하도록 구성되어 있는지 확인합니다.

1. 계정 * > * 연결 * 을 선택합니다.
2. 연결 설정 * 에서 프록시 설정을 확인하십시오.

단계

1. Astra Control Center UI의 * 지원 * 페이지에 나열된 라이센스 일련 번호를 사용하여 NSS 포털에서 케이스를 생성합니다.
2. Astra Control Center UI를 사용하여 지원 번들을 생성하려면 다음 단계를 수행하십시오.
   a. 지원 * 페이지의 지원 번들 타일에서 * 생성 * 을 선택합니다.
   b. 지원 번들 생성 * 창에서 기간을 선택합니다.

      빠른 시간 또는 사용자 지정 시간 계획 중에서 선택할 수 있습니다.

      > 사용자 지정 날짜 범위를 선택하고 날짜 범위 동안 사용자 지정 기간을 지정할 수 있습니다.

   c. 선택한 후 * Confirm * (확인 *)을 선택합니다.
   d. 생성 시 NetApp Support 사이트에 번들 업로드 * 확인란을 선택합니다.
   e. Generate Bundle * 를 선택합니다.

      지원 번들이 준비되면 알림 영역의 * 계정 * > * 알림 * 페이지, * 활동 * 페이지 및 알림 목록(UI 오른쪽 상단에 있는 아이콘을 선택하여 액세스 가능)에 알림이 표시됩니다.

   생성에 실패하면 Generate Bundle(번들 생성) 페이지에 아이콘이 나타납니다. 메시지를 보려면 아이콘을 선택합니다.

> UI 오른쪽 위에 있는 알림 아이콘은 지원 번들과 관련된 이벤트(예: 번들이 성공적으로 생성된 경우, 번들 생성에 실패한 경우, 번들을 업로드할 수 없는 경우, 번들을 다운로드할 수 없는 경우 등)에 대한 정보를 제공합니다.

공기 박기 설치가 있는 경우

공기 교환 설치가 있는 경우 지원 번들을 생성한 후 다음 단계를 수행하십시오. 번들을 다운로드할 수 있는 경우 * Support * 페이지의 * Support Bundles * 섹션에서 * Generate * 옆에 다운로드 아이콘이 나타납니다.

단계

1. 번들을 로컬로 다운로드하려면 다운로드 아이콘을 선택합니다.
2. NSS에 번들을 수동으로 업로드합니다.

   다음 방법 중 하나를 사용하여 이 작업을 수행할 수 있습니다.

   - 사용 "NetApp 인증된 파일 업로드(로그인 필요)".
   - NSS에서 케이스에 번들을 직접 부착합니다.
   - NetApp Active IQ 사용

자세한 내용을 확인하십시오

- "NetApp에 파일을 업로드하는 방법(로그인 필요)"
- "파일을 NetApp에 수동으로 업로드하는 방법(로그인 필요)"

이전 버전의 **Astra Control Center** 문서

이전 릴리스에 대한 문서를 사용할 수 있습니다.

- "Astra Control Center 22.04 문서"
- "Astra Control Center 21.12 문서"
- "Astra Control Center 21.08 문서"

법적 고지

법적 고지 사항은 저작권 선언, 상표, 특허 등에 대한 액세스를 제공합니다.

저작권

"https://www.netapp.com/company/legal/copyright/"

상표

NetApp, NetApp 로고, NetApp 상표 페이지에 나열된 마크는 NetApp Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

"https://www.netapp.com/company/legal/trademarks/"

특허

NetApp 소유 특허 목록은 다음 사이트에서 확인할 수 있습니다.

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

개인 정보 보호 정책

"https://www.netapp.com/company/legal/privacy-policy/"

오픈 소스

통지 파일은 NetApp 소프트웨어에 사용된 타사의 저작권 및 라이센스에 대한 정보를 제공합니다.

- "Astra Control Center에 대한 고지 사항"
- "Astra Data Store에 대한 고지 사항"

Astra Control API 라이센스

https://docs.netapp.com/us-en/astra-automation/media/astra-api-license.pdf