使用 **Astra** 控制中心

Astra Control Center

NetApp
November 21, 2023

目录

使用 Astra 控制中心

开始管理应用程序

你先请 "将集群添加到 Astra Control 管理中"、您可以在集群上安装应用程序(在Astra Control之外)、然后转到Astra Control中的应用程序页面来定义应用程序及其资源。

应用程序管理要求

Astra Control 具有以下应用程序管理要求：

- 许可：要使用Astra Control Center管理应用程序，您需要嵌入式Astra Control Center评估许可证或完整许可证。
- 命名空间：可以使用Astra Control在单个集群上的一个或多个指定命名空间内定义应用程序。一个应用程序可以包含跨越同一集群中多个命名空间的资源。Astra Control不支持在多个集群之间定义应用程序。
- 存储类：如果您安装的应用程序明确设置了存储类、并且需要克隆该应用程序、则克隆操作的目标集群必须具有最初指定的存储类。将具有显式设置的存储类的应用程序克隆到没有相同存储类的集群将失败。
- * Kubernetes Resources* ：使用非 Astra Control 收集的 Kubernetes 资源的应用程序可能没有完整的应用程序数据管理功能。Astra Control 收集以下 Kubernetes 资源：

ClusterRole	ClusterRoleBinding	ConfigMap
CronJob	CustomResourceDefinition	CustomResource
DaemonSet	DeploymentConfig	HorizontalPodAutoscaler
Ingress	MutatingWebhook	NetworkPolicy
PersistentVolumeClaim	Pod	PodDisruptionBudget
PodTemplate	ReplicaSet	Role
RoleBinding	Route	Secret
Service	ServiceAccount	StatefulSet
ValidatingWebhook		

支持的应用程序安装方法

Astra Control 支持以下应用程序安装方法：

- * 清单文件 * ： Astra Control 支持使用 kubectl 从清单文件安装的应用程序。例如：

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

- * Helm 3* ：如果使用 Helm 安装应用程序，则 Astra Control 需要 Helm 版本 3 。完全支持管理和克隆随 Helm 3 安装的应用程序（或从 Helm 2 升级到 Helm 3 ）。不支持管理随 Helm 2 安装的应用程序。
- 操作员部署的应用程序：Astra Control支持使用命名空间范围的操作符安装的应用程序，这些操作符通常采

用"传递值"而不是"传递参考"架构设计。操作员及其安装的应用程序必须使用相同的命名空间；您可能需要为操作员修改部署YAML文件、以确保情况确实如此。

以下是一些遵循这些模式的操作员应用程序：

- "Apache K8ssandra"

> 对于K8ssand拉、支持就地还原操作。要对新命名空间或集群执行还原操作，需要关闭应用程序的原始实例。这是为了确保传输的对等组信息不会导致跨实例通信。不支持克隆应用程序。

- "Jenkins CI"
- "Percona XtraDB 集群"

Astra Control可能无法克隆使用"按参考传递"架构设计的运算符(例如CockroachDB运算符)。在这些类型的克隆操作期间，克隆的操作员会尝试引用源操作员提供的 Kubernetes 机密，尽管在克隆过程中他们拥有自己的新机密。克隆操作可能会失败，因为 Astra Control 不知道源运算符中的 Kubernetes 密钥。

在集群上安装应用程序

你先请 "已添加集群" 对于Astra Control、您可以在集群上安装应用程序或管理现有应用程序。可以管理范围限定为一个或多个命名空间的任何应用程序。

定义应用程序

在Astra Control发现集群上的命名空间后、您可以定义要管理的应用程序。您可以选择 管理跨越一个或多个命名空间的应用程序 或 将整个命名空间作为一个应用程序进行管理。这一切都可以细化到数据保护操作所需的粒度级别。

虽然您可以使用Astra Control单独管理层次结构的两个级别(命名空间和该命名空间中的应用程序或跨命名空间)、但最佳做法是选择一个或另一个。如果在命名空间和应用程序级别同时执行操作，则在 Astra Control 中执行的操作可能会失败。

> 例如、您可能希望为"Maria"设置一个每周节奏的备份策略、但您可能需要比该策略更频繁地备份"MariaDB"(位于同一命名空间中)。根据这些需求、您需要单独管理这些应用程序、而不是作为单命名空间应用程序来管理。

开始之前

- 已将Kubernetes集群添加到Astra Control中。
- 集群上安装的一个或多个应用程序。 阅读有关支持的应用程序安装方法的更多信息。
- 已添加到Astra Control的Kubernetes集群上的现有命名空间。
- (可选) Any上的Kubernetes标签 "支持的Kubernetes资源"。

> 标签是一个键 / 值对，您可以将其分配给 Kubernetes 对象进行标识。通过标签，可以更轻松地对 Kubernetes 对象进行排序，组织和查找。要了解有关 Kubernetes 标签的更多信息， "请参见 Kubernetes 官方文档"。

关于此任务

- 开始之前、您还应了解相关信息 "管理标准命名空间和系统命名空间"。
- 如果您计划在Astra Control中对应用程序使用多个命名空间、 "修改具有命名空间限制的用户角色" 升级到支持多命名空间的Astra Control Center版本后。
- 有关如何使用 Astra Control API 管理应用程序的说明，请参见 "Astra Automation 和 API 信息"。

应用程序管理选项

- [定义要作为应用程序进行管理的资源]
- [定义要作为应用程序进行管理的命名空间]

定义要作为应用程序进行管理的资源

您可以指定 "构成应用程序的Kubernetes资源" 要使用Astra Control进行管理的。通过定义应用程序、您可以将Kubernetes集群中的元素分组到一个应用程序中。此Kubernetes资源集合按命名空间和标签选择器标准进行组织。

通过定义应用程序、您可以更精细地控制要包含在Astra Control操作中的内容、包括克隆、快照和备份。

定义应用程序时、请确保不在具有保护策略的多个应用程序中包含Kubernetes资源。Kubernetes资源上重叠的保护策略可能会发生发生原因 数据冲突。 阅读示例中的更多内容。

阅读有关将集群范围的资源添加到应用程序命名空间的更多信息。

除了自动包含的Astra Control之外、您还可以导入与命名空间资源关联的集群资源。您可以添加一个规则、该规则将包含特定组的资源、种类、版本以及标签(可选)。如果存在Astra Control不会自动包含的资源、您可能需要执行此操作。

您不能排除Astra Control自动包含的任何集群范围的资源。

您可以添加以下内容 `apiVersions` (这些组与API版本结合使用)：

资源种类	**apiVersions (组+版本)**
`ClusterRole`	rbac.authorization.k8s.io/v1
`ClusterRoleBinding`	rbac.authorization.k8s.io/v1
`CustomResource`	apiextensions.k8s.io/v1、apiextensions.k8s.io/v1bea1
`CustomResourceDefinition`	apiextensions.k8s.io/v1、apiextensions.k8s.io/v1bea1
`MutatingWebhookConfiguration`	可批准registration.K8s.IO/v1
`ValidatingWebhookConfiguration`	可批准registration.K8s.IO/v1

步骤

1. 从应用程序页面中、选择*定义*。
2. 在*定义应用程序*窗口中、输入应用程序名称。

3. 在*集群*下拉列表中选择运行应用程序的集群。
4. 从*命名空间*下拉列表中为应用程序选择一个命名空间。

   可以使用Astra Control在单个集群上的一个或多个指定命名空间中定义应用程序。一个应用程序可以包含跨越同一集群中多个命名空间的资源。Astra Control不支持在多个集群之间定义应用程序。

5. (可选)为每个命名空间中的Kubernetes资源输入一个标签。您可以指定单个标签或标签选择器条件(查询)。

   要了解有关 Kubernetes 标签的更多信息， "请参见 Kubernetes 官方文档"。

6. (可选)通过选择*添加命名空间*并从下拉列表中选择命名空间来为应用程序添加其他命名空间。
7. (可选)为您添加的任何其他命名空间输入单个标签或标签选择器条件。
8. (可选)要在Astra Control自动包含的资源之外还包括集群范围的资源、请选中*包括其他集群范围的资源*并完成以下操作：
   a. 选择*添加包含规则*。
   b. 组：从下拉列表中、选择API资源组。
   c. 种类：从下拉列表中、选择对象架构的名称。
   d. 版本：输入API版本。
   e. 标签选择器：也可以包括要添加到规则中的标签。此标签仅用于检索与此标签匹配的资源。如果不提供标签、则Astra Control将收集为该集群指定的所有资源类型的实例。
   f. 查看根据条目创建的规则。
   g. 选择 * 添加 * 。

      您可以根据需要创建任意数量的集群范围资源规则。这些规则将显示在"定义应用程序摘要"中。

9. 选择 * 定义 * 。
10. 选择*定义*后、根据需要对其他应用程序重复此过程。

定义完应用程序后、该应用程序将显示在中 `Healthy` 在应用程序页面上的应用程序列表中的状态。现在、您可以克隆它并创建备份和快照。

您刚刚添加的应用程序在 " 受保护 " 列下可能会显示一个警告图标，表示它尚未备份，并且尚未计划备份。

要查看特定应用程序的详细信息，请选择应用程序名称。

要查看添加到此应用程序的资源、请选择*资源*选项卡。在资源列中选择资源名称后面的数字、或者在搜索中输入资源名称、以查看包含的其他集群范围资源。

定义要作为应用程序进行管理的命名空间

您可以通过将命名空间的资源定义为应用程序来将命名空间中的所有Kubernetes资源添加到Astra Control管理

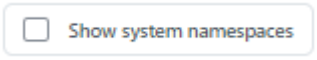
中。如果您要以类似的方式并以通用间隔管理和保护特定命名空间中的所有资源、则此方法比单独定义应用程序更好。

步骤

1. 从集群页面中、选择一个集群。
2. 选择*命名空间*选项卡。
3. 选择包含要管理的应用程序资源的命名空间的"Actions"菜单、然后选择*定义为应用程序*。

如果要定义多个应用程序、请从命名空间列表中进行选择、然后选择左上角的*操作*按钮并选择*定义为应用程序*。这将在各个命名空间中定义多个单独的应用程序。有关多命名空间应用程序、请参见 [定义要作为应用程序进行管理的资源]。

选中*显示系统命名空间*复选框以显示默认情况下在应用程序管理中不使用的系统命名空间。



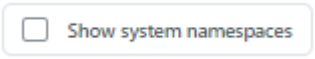
"阅读更多内容"。

此过程完成后、与此命名空间关联的应用程序将显示在中 `Associated applications` 列。

系统命名空间如何?

Astra Control还会发现Kubernetes集群上的系统命名空间。默认情况下、我们不会向您显示这些系统命名空间、因为您很少需要备份系统应用程序资源。

通过选中*显示系统命名空间*复选框、您可以从选定集群的命名空间选项卡中显示系统命名空间。



Astra Control 本身不是一个标准应用程序，而是一个 " 系统应用程序 " 。 您不应尝试管理 Astra Control 本身。默认情况下，用于管理的 Astra Control 本身不会显示。

示例：不同版本的单独保护策略

在此示例中、DevOps团队正在管理"金丝利"版本部署。该团队的集群中有三个Pod运行nginx。其中两个 Pod 专用于稳定版本。第三个 POD 适用于加那利版本。

开发运营团队的Kubernetes管理员会添加此标签 `deployment=stable` 稳定释放Pod。该团队将添加此标签 `deployment=canary` 加那利释放POD。

该团队的稳定版本要求每小时创建一次快照，每天进行备份。金那利版本更短暂、因此他们希望为任何标记的对象创建一个不太积极的短期保护策略 `deployment=canary`。

为了避免可能发生的数据冲突、管理员将创建两个应用程序：一个用于"加那利"版本、一个用于"稳定"版本。这样就可以使两组 Kubernetes 对象的备份，快照和克隆操作分开。

了解更多信息

- "使用 Astra Control API"

- "取消管理应用程序"

保护应用程序

保护概述

您可以使用 Astra 控制中心为应用程序创建备份，克隆，快照和保护策略。备份应用程序可帮助您的服务和关联数据尽可能地可用；在灾难情形下，从备份还原可以确保应用程序及其关联数据的完全恢复，而不会造成任何中断。备份，克隆和快照有助于防止常见威胁，例如勒索软件，意外数据丢失和环境灾难。 "了解 Astra 控制中心提供的数据保护类型以及何时使用"。

此外、您还可以将应用程序复制到远程集群、以便为灾难恢复做好准备。

应用程序保护工作流

您可以使用以下示例工作流开始保护应用程序。

[一个] 保护所有应用程序

要确保您的应用程序立即受到保护， "为所有应用程序创建手动备份"。

[两个] 为每个应用程序配置一个保护策略

要自动执行未来备份和快照， "为每个应用程序配置一个保护策略"。例如，您可以从每周备份和每日快照开始，这两种备份均保留一个月。强烈建议使用保护策略自动执行备份和快照，而不是手动备份和快照。

[三个] 调整保护策略

随着应用程序及其使用模式的变化，根据需要调整保护策略以提供最佳保护。

[四个] 将应用程序复制到远程集群

"复制应用程序" 使用NetApp SnapMirror技术连接到远程集群。Astra Control可将快照复制到远程集群、从而提供异步灾难恢复功能。

[五个] 发生灾难时、请使用最新备份或复制功能将应用程序还原到远程系统

如果发生数据丢失，您可以通过进行恢复 "还原最新备份" 每个应用程序的第一个。然后，您可以还原最新的快照（如果可用）。或者、您也可以使用复制到远程系统。

通过快照和备份保护应用程序

通过使用自动保护策略或临时创建快照和备份来保护所有应用程序。您可以使用Astra控制中心UI或 "Astra Control API" 保护应用程序。

关于此任务

- * Helm部署的应用程序*：如果您使用Helm部署应用程序、则Astra控制中心需要Helm版本3。完全支持管理和克隆使用 Helm 3 部署的应用程序（或从 Helm 2 升级到 Helm 3 ）。不支持使用 Helm 2 部署的应用程

序。

- **(仅限OpenShift集群)**添加策略：在OpenShift集群上创建用于托管应用程序的项目时、系统会为该项目(或Kubernetes命名空间)分配一个SecurityContext UID。要使 Astra 控制中心能够保护您的应用程序并将应用程序移动到 OpenShift 中的其他集群或项目，您需要添加策略，使应用程序能够作为任何 UID 运行。例如，以下 OpenShift 命令行界面命令会为 WordPress 应用程序授予相应的策略。

```
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
```

您可以执行以下与保护应用程序数据相关的任务：

- [配置保护策略]
- [创建快照]
- [创建备份]
- [查看快照和备份]
- [删除快照]
- [取消备份]
- [删除备份]

配置保护策略

保护策略通过按定义的计划创建快照，备份或这两者来保护应用程序。您可以选择每小时，每天，每周和每月创建快照和备份，并且可以指定要保留的副本数。

如果您需要备份或快照的运行频率高于每小时一次，则可以 "使用 Astra Control REST API 创建快照和备份"。

偏移备份和复制计划以避免计划重叠。例如、在每小时的前几个小时执行备份、并计划复制、以5分钟的偏移和10分钟的间隔开始。

如果您的应用使用由支持的存储类 `ontap-nas-economy` 驱动程序、无法使用保护策略。如果要计划备份和快照、请迁移到Asta Control支持的存储类。

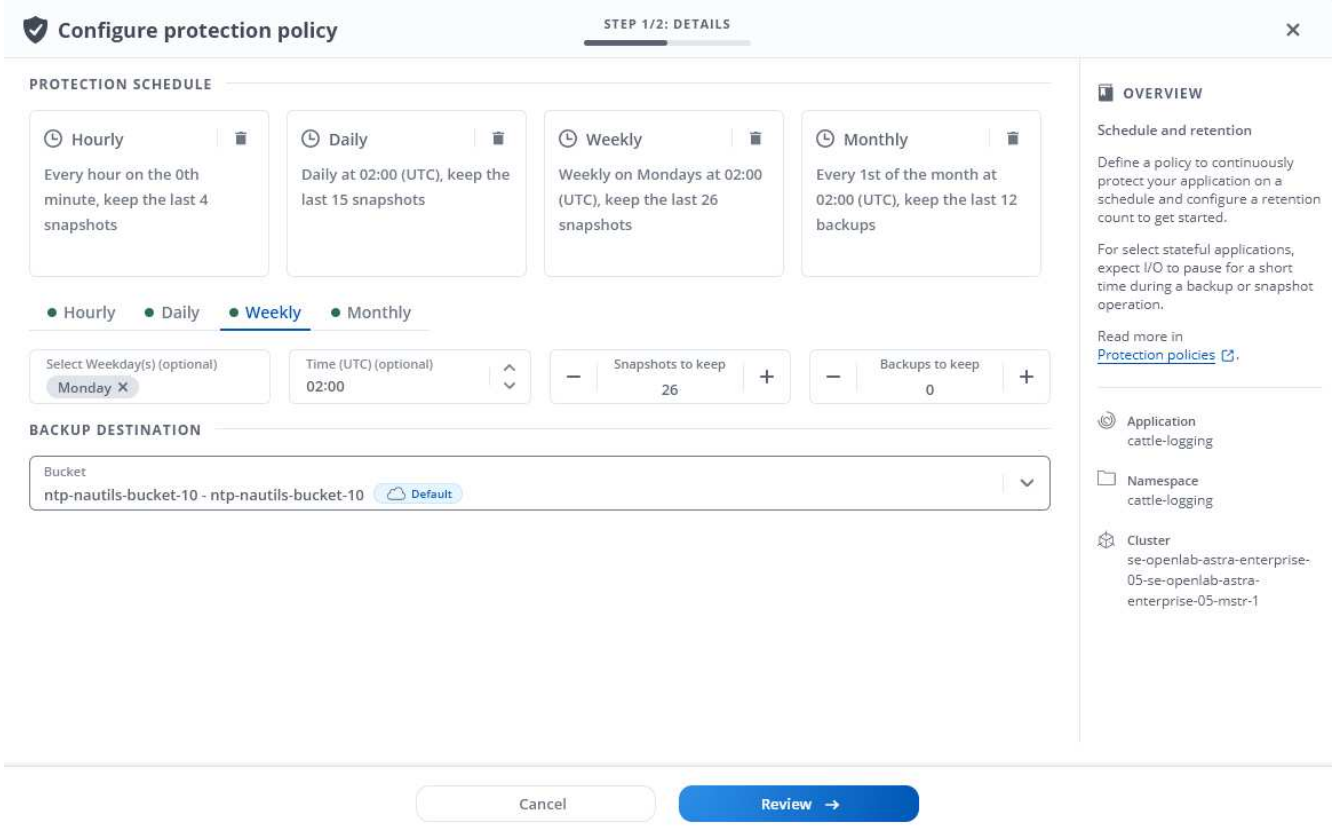
步骤

1. 选择 * 应用程序 * ，然后选择应用程序的名称。
2. 选择 * 数据保护 * 。
3. 选择 * 配置保护策略 * 。
4. 通过选择每小时，每天，每周和每月保留的快照和备份数量来定义保护计划。

   您可以同时定义每小时，每天，每周和每月计划。在设置保留级别之前，计划不会变为活动状态。

   在为备份设置保留级别时，您可以选择要将备份存储到的存储分段。

   以下示例将为快照和备份设置四个保护计划：每小时，每天，每周和每月。



5. 选择 * 审阅 * 。
6. 选择 * 设置保护策略。 *

结果

Astra Control 通过使用您定义的计划和保留策略创建和保留快照和备份来实施数据保护策略。

创建快照

您可以随时创建按需快照。

> 如果您的应用使用由支持的存储类 `ontap-nas-economy` 驱动程序、无法创建快照。为快照使用备用存储类。

步骤

1. 选择 * 应用程序 * 。
2. 从所需应用程序的 * 操作 * 列的选项菜单中，选择 * 快照 * 。
3. 自定义快照的名称、然后选择*下一步*。
4. 查看快照摘要并选择 * 快照 * 。

结果

快照过程开始。如果在*数据保护*>*快照*页面的*状态*列中、快照状态为*运行状况*、则快照将成功。

创建备份

您也可以随时备份应用程序。

> Astra 控制中心中的 S3 存储分段不会报告可用容量。在备份或克隆由 Astra 控制中心管理的应用程序之前，请检查 ONTAP 或 StorageGRID 管理系统中的存储分段信息。

> 如果您的应用使用由支持的存储类 `ontap-nas-economy` 驱动程序、请确保您已定义 `backendType` 中的参数 "Kubbernetes存储对象" 值为 `ontap-nas-economy` 在执行任何保护操作之前。备份由支持的应用程序 `ontap-nas-economy` 会造成系统中断、应用程序将不可用、直到备份操作完成。

步骤

1. 选择 * 应用程序 * 。
2. 从所需应用程序的*操作*列的选项菜单中、选择*备份*。
3. 自定义备份的名称。
4. 选择是否从现有快照备份应用程序。如果选择此选项，则可以从现有快照列表中进行选择。
5. 从存储分段列表中为备份选择一个目标分段。
6. 选择 * 下一步 * 。
7. 查看备份摘要并选择*备份*。

结果

Astra Control 会创建应用程序的备份。

> 如果网络发生中断或异常缓慢，备份操作可能会超时。这会导致备份失败。

> 如果需要取消正在运行的备份、请按照中的说明进行操作 [取消备份]。要删除备份、请等待备份完成、然后按照中的说明进行操作 [删除备份]。

> 在执行数据保护操作（克隆，备份，还原）并随后调整永久性卷大小后，在 UI 中显示新卷大小之前，最长会有 20 分钟的延迟。数据保护操作将在几分钟内成功完成，您可以使用存储后端的管理软件确认卷大小的更改。

查看快照和备份

您可以从数据保护选项卡查看应用程序的快照和备份。

步骤

1. 选择 * 应用程序 * ，然后选择应用程序的名称。
2. 选择 * 数据保护 * 。

   默认情况下会显示快照。

3. 选择 * 备份 * 可查看备份列表。

删除快照

删除不再需要的计划快照或按需快照。

> 您不能删除当前正在复制的快照。

步骤

1. 选择 * 应用程序 * ，然后选择受管应用程序的名称。
2. 选择 * 数据保护 * 。
3. 从选项菜单的 * 操作 * 列中为所需快照选择 * 删除快照 * 。
4. 键入单词 "delete" 确认删除，然后选择 * 是，删除 snapshot* 。

结果

Astra Control 会删除快照。

取消备份

您可以取消正在进行的备份。

> 要取消备份、备份必须位于中 `Running` 状态。您无法取消中的备份 `Pending` 状态。

步骤

1. 选择 * 应用程序 * ，然后选择应用程序的名称。
2. 选择 * 数据保护 * 。
3. 选择 * 备份 * 。
4. 从选项菜单中的*操作*列中为所需备份选择*取消*。
5. 键入单词"cancel"以确认操作、然后选择*是、取消备份*。

删除备份

删除不再需要的计划备份或按需备份。

> 如果需要取消正在运行的备份、请按照中的说明进行操作 [取消备份]。要删除备份、请等待备份完成、然后按照以下说明进行操作。

步骤

1. 选择 * 应用程序 * ，然后选择应用程序的名称。
2. 选择 * 数据保护 * 。
3. 选择 * 备份 * 。
4. 从选项菜单的 * 操作 * 列中为所需备份选择 * 删除备份 * 。
5. 键入单词 "delete" 确认删除，然后选择 * 是，删除备份 * 。

结果

Astra Control 会删除备份。

还原应用程序

Astra Control 可以从快照或备份还原应用程序。将应用程序还原到同一集群时，从现有快照进行还原的速度会更快。您可以使用 Astra Control UI 或 "Astra Control API" 还原应用程序。

> 如果将命名空间筛选器添加到在还原或克隆操作之后运行的执行挂钩、并且还原或克隆源和目标位于不同的命名空间中、则命名空间筛选器仅会应用于目标命名空间。

关于此任务

- 首先保护您的应用程序：强烈建议您在恢复应用程序之前为其创建快照或备份。这样、您可以在还原失败时从快照或备份克隆。
- 检查目标卷：如果要还原到其他存储类、请确保该存储类使用相同的永久性卷访问模式(例如ReadWriteMany)。如果目标永久性卷访问模式不同，还原操作将失败。例如、如果源永久性卷使用rwx访问模式、请选择无法提供rwx的目标存储类、例如Azure托管磁盘、AWS EBS、Google持久磁盘或 `ontap-san`，发生原因则还原操作是否会失败。有关永久性卷访问模式的详细信息、请参阅 "Kubernetes" 文档。
- 规划空间需求：对使用NetApp ONTAP 存储的应用程序执行原位还原时、还原的应用程序使用的空间可能会增加一倍。执行原位还原后、从还原的应用程序中删除所有不需要的快照以释放存储空间。
- **(仅限OpenShift集群)**添加策略：在OpenShift集群上创建用于托管应用程序的项目时、系统会为该项目(或Kubernetes命名空间)分配一个SecurityContext UID。要使 Astra 控制中心能够保护您的应用程序并将应用程序移动到 OpenShift 中的其他集群或项目，您需要添加策略，使应用程序能够作为任何 UID 运行。例如，以下 OpenShift 命令行界面命令会为 WordPress 应用程序授予相应的策略。

```
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
```

- * Helm部署的应用程序*：完全支持使用Helm 3部署的应用程序(或从Helm 2升级到Helm 3)。不支持使用 Helm 2 部署的应用程序。

> 在与其他应用程序共享资源的应用程序上执行原位还原操作可能会产生意外结果。对其中一个应用程序执行原位还原时、这些应用程序之间共享的任何资源都会被替换。有关详细信息，请参见此示例。

步骤

1. 选择 * 应用程序 * ，然后选择应用程序的名称。
2. 从“操作”列的“选项”菜单中，选择*Restore*。
3. 选择还原类型：
   - 还原到原始命名空间：使用此操作步骤 将应用程序原位还原到原始集群。

     > 如果您的应用使用由支持的存储类 `ontap-nas-economy` 驱动程序、则必须使用原始存储类还原应用程序。如果要将应用程序还原到同一命名空间、则不能指定其他存储类。

     i. 选择要用于原位还原应用程序的快照或备份、这会将应用程序还原到其自身的早期版本。

ii. 选择 * 下一步 * 。

> 如果还原到先前已删除的命名空间、则在还原过程中会创建一个同名的新命名空间。任何有权管理先前删除的命名空间中的应用程序的用户都需要手动还原对新重新创建的命名空间的权限。

◦ 还原到新命名空间：使用此操作步骤 将应用程序还原到另一个集群或使用与源不同的命名空间。

> 您可以使用此操作步骤 执行以下任一操作 存储类 `ontap-nas` 在同一集群*或*上、将应用程序复制到存储类由支持的另一集群 `ontap-nas-economy` 驱动程序。

i. 指定已还原应用程序的名称。

ii. 为要还原的应用程序选择目标集群。

iii. 为与应用程序关联的每个源命名空间输入目标命名空间。

> 作为此还原选项的一部分、Astra Control会创建新的目标命名空间。指定的目标命名空间不能已存在于目标集群上。

iv. 选择 * 下一步 * 。

v. 选择用于还原应用程序的快照或备份。

vi. 选择 * 下一步 * 。

vii. 选择以下选项之一：

- 使用原始存储类还原：除非目标集群上不存在、否则应用程序将使用最初关联的存储类。在这种情况下、将使用集群的默认存储类。
- 使用其他存储类还原：选择目标集群上的存储类。在还原过程中、所有应用程序卷(无论其最初关联的存储类是什么)都将迁移到此不同的存储类。

viii. 选择 * 下一步 * 。

4. 选择要筛选的任何资源：

◦ 恢复所有资源：恢复与原始应用程序关联的所有资源。

◦ 过滤资源：指定规则以还原原始应用程序资源的子集：

i. 选择在已还原的应用程序中包括或排除资源。

ii. 选择*添加包含规则*或*添加排除规则*，并配置规则以在应用程序恢复期间过滤正确的资源。您可以编辑或删除规则、然后重新创建规则、直到配置正确为止。

> 要了解有关配置包含和排除规则的信息、请参见 [在应用程序还原期间筛选资源]。

5. 选择 * 下一步 * 。

6. 请仔细查看有关还原操作的详细信息，键入“restore”(如果出现提示)，然后选择*Restore*。

结果

Astra Control 会根据您提供的信息还原应用程序。如果您已原位还原应用程序、则现有永久性卷的内容将替换为已还原应用程序中的永久性卷的内容。

在执行数据保护操作(克隆、备份或还原)并随后调整永久性卷大小后、在Web UI中显示新卷大小之前、最多会有20分钟的延迟。数据保护操作将在几分钟内成功完成，您可以使用存储后端的管理软件确认卷大小的更改。

任何按命名空间名称/ID或命名空间标签限制命名空间的成员用户都可以将应用程序克隆或还原到同一集群上的新命名空间或其组织帐户中的任何其他集群。但是，同一用户无法访问新命名空间中的克隆或还原应用程序。通过克隆或还原操作创建新命名空间后，帐户管理员 / 所有者可以编辑成员用户帐户并更新受影响用户的角色约束，以授予对新命名空间的访问权限。

在应用程序还原期间筛选资源

您可以向添加筛选器规则 "还原" 此操作将指定要从还原的应用程序中包括或排除的现有应用程序资源。您可以根据指定的命名空间、标签或GVK (GroupVersion Kind)包括或排除资源。

阅读有关包含和排除方案的更多信息

- 选择包含原始命名空间的规则(就地还原)：您在规则中定义的现有应用程序资源将被删除，并替换为用于还原的选定快照或备份中的应用程序资源。未在包含规则中指定的任何资源将保持不变。
- 选择包含新名称空间的规则：使用此规则在还原的应用程序中选择所需的特定资源。未在包含规则中指定的任何资源将不会包含在已还原的应用程序中。
- 选择包含原始名称空间的排除规则(就地恢复)：您指定要排除的资源将不会还原、并且保持不变。未指定排除的资源将从快照或备份中还原。如果筛选的资源中包含相应的状态集、则永久性卷上的所有数据都将被删除并重新创建。
- 选择包含新名称空间的排除规则：使用此规则可选择要从还原的应用程序中删除的特定资源。未指定排除的资源将从快照或备份中还原。

规则可以是包含类型、也可以是排除类型。不提供组合使用资源包含和排除的规则。

步骤

1. 选择筛选资源并在恢复应用程序向导中选择包含或排除选项后，选择*添加包含规则*或*添加排除规则*。

   您不能排除Asta Control自动包含的任何集群范围的资源。

2. 配置筛选器规则：

   必须至少指定一个命名空间、标签或GVK。确保在应用筛选器规则后保留的任何资源足以使已还原的应用程序保持运行状况良好。

   a. 为规则选择特定命名空间。如果不进行选择、则会在筛选器中使用所有名称空间。

      如果您的应用程序最初包含多个名称空间、而您将其还原到新的名称空间、则会创建所有名称空间、即使它们不包含资源也是如此。

   b. (可选)输入资源名称。

   c. (可选)标签选择器：包括A "标签选择器" 以添加到规则中。标签选择器用于仅筛选与选定标签匹配的资源。

d. (可选)选择*使用GVK (GroupVersion Kind)设置来筛选资源*以获取其他筛选选项。

> 如果使用GVK筛选器、则必须指定版本和种类。

i. (可选)组：从下拉列表中选择Kubernetes API组。

ii. **KND**：从下拉列表中选择要在筛选器中使用的Kubernetes资源类型的对象模式。

iii. 版本：选择Kubernetes API版本。

3. 查看根据条目创建的规则。
4. 选择 * 添加 * 。

> 您可以根据需要创建任意数量的资源包含和排除规则。这些规则将显示在启动操作之前的还原应用程序摘要中。

从**ONTAP**经济型存储迁移到**ONTAP NAS**存储

您可以使用Astra控件 "应用程序还原" 或 "应用程序克隆" 从支持的存储类迁移应用程序卷的操作 `ontap-nas-economy`，允许对支持的存储类使用有限的应用程序保护选项 `ontap-nas` 提供全系列A作用 力控制保护选项。克隆或还原操作会迁移使用的基于qtree的卷 `ontap-nas-economy` 后端到由支持的标准卷 `ontap-nas`。卷、而不管它们是不是 `ontap-nas-economy` 仅备份或混合备份、将迁移到目标存储类。迁移完成后、保护选项将不再受限。

如果某个应用程序与其他应用程序共享资源、则就地恢复会变得非常复杂

您可以对与其他应用共享资源并产生意外结果的应用程序执行原位还原操作。对其中一个应用程序执行原位还原时、这些应用程序之间共享的任何资源都会被替换。

以下示例情形会在使用NetApp SnapMirror复制进行还原时产生不希望出现的情况：

1. 您可以定义应用程序 `app1` 使用命名空间 `ns1`。
2. 您可以为配置复制关系 `app1`。
3. 您可以定义应用程序 `app2` (在同一集群上)使用命名空间 `ns1` 和 `ns2`。
4. 您可以为配置复制关系 `app2`。
5. 反向复制 `app2`。这将导致 `app1` 要停用的源集群上的应用程序。

使用**SnapMirror**技术将应用程序复制到远程系统

使用Astra Control、您可以使用NetApp SnapMirror技术的异步复制功能、以低RPO (恢复点目标)和低RTO (恢复时间目标)为应用程序构建业务连续性。配置完成后、应用程序便可将数据和应用程序更改从一个集群复制到另一个集群。

有关备份/还原与复制之间的比较、请参见 "数据保护概念"。

您可以在不同情形下复制应用程序、例如以下仅限内部部署、混合和多云情形：

- 内部站点A到内部站点B

- 使用Cloud Volumes ONTAP 从内部部署到云
- 采用Cloud Volumes ONTAP 的云到内部部署
- 采用Cloud Volumes ONTAP 的云到云(在同一云提供商的不同区域之间或不同云提供商之间)

Astra Control可以跨内部集群、内部到云(使用Cloud Volumes ONTAP)或云之间(Cloud Volumes ONTAP到Cloud Volumes ONTAP)复制应用程序。

您可以同时按相反方向复制另一个应用程序(在另一个集群或站点上运行)。例如、应用程序A、B、C可以从数据中心1复制到数据中心2；应用程序X、Y、Z可以从数据中心2复制到数据中心1。

使用Astra Control、您可以执行以下与复制应用程序相关的任务：

- [设置复制关系]
- [在目标集群上使复制的应用程序联机(故障转移)]
- [重新同步故障转移复制]
- [反向复制应用程序]
- [将应用程序故障恢复到原始源集群]
- [删除应用程序复制关系]

复制前提条件

Astra Control应用程序复制要求在开始之前满足以下前提条件：

- * ONTAP集群*：
  - **Trident**：使用ONTAP作为后端的源和目标Kubernetes集群上必须同时存在Astra Drident版本22.07或更高版本。
  - 许可证：必须在源和目标ONTAP集群上启用使用数据保护包的ONTAP SnapMirror异步许可证。请参见 "ONTAP 中的SnapMirror许可概述" 有关详细信息 …
- 配对：
  - 集群和**SVM**：ONTAP集群和主机SVM必须配对。请参见 "集群和 SVM 对等概述" 有关详细信息 …
  - 三 端到端和**SVM**：配对的远程SVM必须可供目标集群上的Astra三端到端使用。
- **Astra**控制中心：

"部署Asta Control Center" 在第三个故障域或二级站点中、以实现无缝灾难恢复。

  - 受管集群：必须将以下集群添加到Astra Control并由Astra Control进行管理、最好是在不同的故障域或站点上：
    - 源Kubbernetes集群
    - 目标Kubbernetes集群
    - 关联的ONTAP集群
  - 用户帐户：将ONTAP存储后端添加到Astra控制中心时、请应用具有"admin"角色的用户凭据。此角色具有访问方法 `http` 和 `ontapi` 已在ONTAP 源集群和目标集群上启用。请参见 "管理ONTAP 文档中的用

户帐户" 有关详细信息 …

- **Astra三端/ ONTAP配置**：Astra控制中心要求您至少配置一个支持源集群和目标集群复制的存储类。

> Astra Control复制支持使用单个存储类的应用程序。将应用程序添加到命名空间时、请确保该应用程序与命名空间中的其他应用程序具有相同的存储类。向复制的应用程序添加PVC时、请确保新PVC与命名空间中的其他PVC具有相同的存储类。

设置复制关系

设置复制关系涉及以下方面：

- 选择Astra Control创建应用程序快照的频率(包括应用程序的Kubernetes资源以及应用程序每个卷的卷快照)
- 选择复制计划(包括Kubernetes资源以及永久性卷数据)
- 设置创建快照的时间

步骤

1. 从Astra Control左侧导航栏中、选择*应用程序*。
2. 在应用程序页面中、选择*数据保护*>*复制*选项卡。
3. 在Data Protection > Replication选项卡中、选择*配置复制策略*。或者、从应用程序保护框中、选择操作选项并选择*配置复制策略*。
4. 输入或选择以下信息：
   - 目标集群：输入与源集群不同的目标集群。
   - 目标存储类：选择或输入在目标ONTAP 集群上使用配对SVM的存储类。
   - 复制类型："异步"是当前唯一可用的复制类型。
   - 目标命名空间：为目标集群输入新的或现有的目标命名空间。
   - (可选)通过选择*添加命名空间*并从下拉列表中选择命名空间来添加其他命名空间。
   - 复制频率：设置Astra Control创建Snapshot并将其复制到目标的频率。
   - 偏移：设置从Astra Control创建快照的小时数开始的分钟数。您可能希望使用偏移量、以便它不会与其他计划的操作保持一致。

   > 偏移备份和复制计划以避免计划重叠。例如、在每小时的前几个小时执行备份、并计划复制、以5分钟的偏移和10分钟的间隔开始。

5. 选择*下一步*、查看摘要、然后选择*保存*。

   > 首先、在执行第一个计划之前、状态将显示"app-mirror"。

   Astra Control会创建用于复制的应用程序Snapshot。

6. 要查看应用程序Snapshot状态、请选择*应用程序*>*快照*选项卡。

   Snapshot名称使用的格式 `replication-schedule-<string>`。Astra Control会保留用于复制的最后一个Snapshot。成功完成复制后、所有较早的复制Snapshot都会被删除。

结果

这将创建复制关系。

建立关系后、Astra Control将完成以下操作：

- 在目标上创建命名空间(如果不存在)
- 在目标命名空间上创建与源应用程序的PVC对应的PVC。
- 创建初始应用程序一致的Snapshot。
- 使用初始Snapshot为永久性卷建立SnapMirror关系。

"Data Protection (数据保护)"页面将显示复制关系的状态：
<Health status>|<Relationship life cycle state>

例如：
正常|已建立

在本主题末尾了解有关复制状态和状态的更多信息。

在目标集群上使复制的应用程序联机(故障转移)

使用Astra Control、您可以将复制的应用程序故障转移到目标集群。此操作步骤 将停止复制关系并使应用程序在目标集群上联机。如果应用程序正常运行、则此操作步骤 不会停止源集群上的应用程序。

步骤

1. 从Astra Control左侧导航栏中、选择*应用程序*。
2. 在应用程序页面中、选择*数据保护*>*复制*选项卡。
3. 在"数据保护">"复制"选项卡的"操作"菜单中、选择*故障转移*。
4. 在故障转移页面中、查看相关信息并选择*故障转移*。

结果

故障转移操作步骤后会执行以下操作：

- 在目标集群上、应用程序将基于最新复制的快照启动。
- 源集群和应用程序(如果运行正常)不会停止、并且将继续运行。
- 复制状态将更改为"故障转移"、然后在完成后更改为"故障转移"。
- 根据故障转移时源应用程序上的计划、源应用程序的保护策略将复制到目标应用程序。
- 如果源应用程序启用了一个或多个还原后执行挂钩、则会为目标应用程序运行这些执行挂钩。
- Astra Control会在源集群和目标集群上显示应用程序及其各自的运行状况。

重新同步故障转移复制

重新同步操作将重新建立复制关系。您可以选择关系的源、以便在源或目标集群上保留数据。此操作将重新建立SnapMirror关系、以便按所选方向启动卷复制。

此过程会在重新建立复制之前停止新目标集群上的应用程序。

在重新同步过程中、生命周期状态将显示为"正在建立"。

步骤

1. 从Astra Control左侧导航栏中、选择*应用程序*。
2. 在应用程序页面中、选择*数据保护*>*复制*选项卡。
3. 在"Data Protection">"Replication"选项卡中、从"Actions"菜单中选择*重新同步*。
4. 在重新同步页面中、选择包含要保留的数据的源或目标应用程序实例。

   请仔细选择重新同步源、因为目标上的数据将被覆盖。

5. 选择*重新同步*以继续。
6. 键入"resync-"进行确认。
7. 选择*是、重新同步*以完成。

结果

- 复制页面将显示"正在建立"作为复制状态。
- Astra Control将停止新目标集群上的应用程序。
- Astra Control使用SnapMirror重新同步功能按选定方向重新建立永久性卷复制。
- 复制页面将显示已更新的关系。

反向复制应用程序

这是一项计划内操作、用于将应用程序移动到目标集群、同时继续复制回原始源集群。Astra Control会先停止源集群上的应用程序并将数据复制到目标、然后再将应用程序故障转移到目标集群。

在这种情况下、您将交换源和目标。原始源集群将成为新的目标集群、而原始目标集群将成为新的源集群。

步骤

1. 从Astra Control左侧导航栏中、选择*应用程序*。
2. 在应用程序页面中、选择*数据保护*>*复制*选项卡。
3. 在"Data Protection">"Replication"选项卡中、从"Actions"菜单中选择*反向复制*。
4. 在反向复制页面中、查看相关信息并选择*反向复制*以继续。

结果

反向复制会执行以下操作：

- 将为原始源应用程序的Kubernetes资源创建Snapshot。
- 通过删除原始源应用程序的Kubernetes资源(保留PVC和PV)、可以正常停止原始源应用程序的Pod。
- 关闭Pod后、将创建并复制应用程序卷的快照。
- SnapMirror关系将中断、从而使目标卷做好读/写准备。
- 应用程序的Kubernetes资源会使用在原始源应用程序关闭后复制的卷数据从预关闭的Snapshot进行还原。

- 反向重新建立复制。

将应用程序故障恢复到原始源集群

使用Astra Control、您可以通过以下操作序列在故障转移操作后实现"故障恢复"。在此恢复原始复制方向的工作流中、Astra Control会将所有应用程序更改复制(重新同步)回原始源集群、然后再反转复制方向。

此过程从已完成故障转移到目标的关系开始、涉及以下步骤：

- 从故障转移状态开始。
- 重新同步此关系。
- 反转复制。

步骤

1. 从Astra Control左侧导航栏中、选择*应用程序*。
2. 在应用程序页面中、选择*数据保护*>*复制*选项卡。
3. 在"Data Protection">"Replication"选项卡中、从"Actions"菜单中选择*重新同步*。
4. 对于故障恢复操作、请选择故障转移应用程序作为重新同步操作的源(在故障转移后保留写入的任何数据)。
5. 键入"resync-"进行确认。
6. 选择*是、重新同步*以完成。
7. 重新同步完成后、在"Data Protection">"Replication"选项卡中、从"Actions"菜单中选择*反向复制*。
8. 在反向复制页面中、查看相关信息并选择*反向复制*。

结果

这将合并"重新同步"和"反向关系"操作的结果、以便在复制恢复到原始目标集群的情况下使应用程序在原始源集群上联机。

删除应用程序复制关系

删除此关系会导致出现两个独立的应用程序、它们之间没有任何关系。

步骤

1. 从Astra Control左侧导航栏中、选择*应用程序*。
2. 在应用程序页面中、选择*数据保护*>*复制*选项卡。
3. 在"数据保护">"复制"选项卡的"应用程序保护"框或关系图中、选择*删除复制关系*。

结果

删除复制关系后会执行以下操作：

- 如果已建立此关系、但此应用程序尚未在目标集群上联机(故障转移)、则Astra Control将保留初始化期间创建的PVC、在目标集群上保留一个"空"受管应用程序、并保留目标应用程序以保留可能已创建的任何备份。
- 如果应用程序已在目标集群上联机(故障转移)、则Astra Control会保留PVC和目标应用程序。源应用程序和目标应用程序现在被视为独立的应用程序。备份计划会同时保留在两个应用程序上、但不会彼此关联。

复制关系运行状况和关系生命周期状态

Astra Control显示关系的运行状况以及复制关系的生命周期状态。

复制关系运行状况

以下状态指示复制关系的运行状况：

- 正常：此关系正在建立或已建立、并且已成功传输最新的Snapshot。
- 警告：此关系正在进行故障转移或已进行故障转移(因此不再保护源应用程序)。
- * 严重 *
  - 此关系正在建立或故障转移、上次协调尝试失败。
  - 已建立此关系、上次尝试协调添加新PVC失败。
  - 已建立此关系(因此已成功复制Snapshot、并且可以进行故障转移)、但最近的Snapshot无法复制或无法复制。

复制生命周期状态

以下状态反映了复制生命周期的不同阶段：

- 正在建立：正在创建新的复制关系。Astra Control会根据需要创建命名空间、在目标集群上的新卷上创建永久性卷声明(PVC)、并创建SnapMirror关系。此状态还可以指示复制正在重新同步或反转复制。
- 已建立：存在复制关系。Astra Control会定期检查PVC是否可用、检查复制关系、定期创建应用程序的Snapshot并确定应用程序中的任何新源PVC。如果是、则Astra Control会创建资源以将其包括在复制中。
- 故障转移：Astra Control中断SnapMirror关系、并从上次成功复制的应用程序Snapshot还原应用程序的Kubernetes资源。
- 故障转移：Astra Control停止从源集群复制、在目标上使用最新(成功)复制的应用程序Snapshot、并还原Kubernetes资源。
- 正在重新同步：Astra Control使用SnapMirror重新同步将重新同步源上的新数据重新同步到重新同步目标。此操作可能会根据同步方向覆盖目标上的某些数据。Astra Control会停止在目标命名空间上运行的应用程序、并删除Kubernetes应用程序。在重新同步过程中、状态将显示为正在建立。
- 正在反转：是指在继续复制回原始源集群的同时将应用程序移动到目标集群的计划操作。Astra Control会停止源集群上的应用程序、将数据复制到目标、然后将应用程序故障转移到目标集群。在反向复制期间、状态显示为"正在 建立"。
- 正在删除：
  - 如果已建立复制关系、但尚未进行故障转移、则Astra Control会删除复制期间创建的PVC、并删除目标受管应用程序。
  - 如果复制已失败、则Astra Control会保留PVC和目标应用程序。

克隆和迁移应用程序

您可以克隆现有应用程序、以便在同一个Kubernetes集群或另一个集群上创建重复的应用程序。当 Astra Control 克隆应用程序时，它会为您的应用程序配置和永久性存储创建一个克隆。

如果您需要将应用程序和存储从一个 Kubernetes 集群移动到另一个集群，则克隆可以助您一臂之力。例如，您可能希望通过 CI/CD 管道以及在 Kubernetes 命名空间之间移动工作负载。您可以使用Astra控制中心UI或 "Astra Control API" 克隆和迁移应用程序。

如果将命名空间筛选器添加到在还原或克隆操作之后运行的执行挂钩、并且还原或克隆源和目标位于不同的命名空间中、则命名空间筛选器仅会应用于目标命名空间。

开始之前

- 检查目标卷：如果克隆到其他存储类、请确保该存储类使用相同的永久性卷访问模式(例如ReadWriteMany)。如果目标永久性卷访问模式不同、则克隆操作将失败。例如、如果源永久性卷使用rwx访问模式、请选择无法提供rwx的目标存储类、例如Azure托管磁盘、AWS EBS、Google持久磁盘或 `ontap-san`，发生原因将使克隆操作失败。有关永久性卷访问模式的详细信息、请参阅 "Kubernetes" 文档。
- 要将应用程序克隆到其他集群、您需要确保包含源集群和目标集群(如果不相同)的云实例具有默认分段。您需要为每个云实例分配一个默认分段。
- 在克隆操作期间、需要IngressClass资源或webhooks才能正常运行的应用程序不能在目标集群上定义这些资源。

在 OpenShift 环境中克隆应用程序期间， Astra Control Center 需要允许 OpenShift 挂载卷并更改文件所有权。因此，您需要配置 ONTAP 卷导出策略以允许执行这些操作。您可以使用以下命令执行此操作：

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`

克隆限制

- 显式存储类：如果部署的应用程序已明确设置存储类、并且需要克隆此应用程序、则目标集群必须具有最初指定的存储类。将具有显式设置的存储类的应用程序克隆到没有相同存储类的集群将失败。
- 基于**ONTAP**的**NAS**经济型存储类：如果您的应用使用由支持的存储类 `ontap-nas-economy` 驱动程序、则克隆操作的备份部分会造成系统中断。在备份完成之前、源应用程序不可用。克隆操作的还原部分不会造成系统中断。
- 克隆和用户约束：任何按命名空间名称/ID或命名空间标签限制命名空间的成员用户都可以将应用程序克隆或还原到同一集群上的新命名空间或其组织帐户中的任何其他集群。但是，同一用户无法访问新命名空间中的克隆或还原应用程序。通过克隆或还原操作创建新命名空间后，帐户管理员 / 所有者可以编辑成员用户帐户并更新受影响用户的角色约束，以授予对新命名空间的访问权限。
- 克隆使用默认分段：在应用程序备份或应用程序还原期间、您可以选择指定分段ID。但是，应用程序克隆操作始终使用已定义的默认分段。没有选项可用于更改克隆的分段。如果要控制使用哪个存储分段，您可以选择 "更改存储分段默认值" 或者执行 "backup" 后跟 A "还原" 请单独使用。
- 使用**Jenkins CI**：如果克隆操作员部署的Jenkins CI实例、则需要手动还原持久数据。这是应用程序部署模式的一个限制。
- 对于**S3**存储分段：Astra控制中心中的S3存储分段不报告可用容量。在备份或克隆由 Astra 控制中心管理的应用程序之前，请检查 ONTAP 或 StorageGRID 管理系统中的存储分段信息。

OpenShift 注意事项

- 集群和**OpenShift**版本：如果在集群之间克隆应用程序、则源集群和目标集群必须是OpenShift的相同分发版本。例如，如果从 OpenShift 4.7 集群克隆应用程序，请使用同时也是 OpenShift 4.7 的目标集群。

- 项目和**UID**：在OpenShift集群上创建用于托管应用程序的项目时、系统会为该项目(或Kubernetes命名空间)分配一个SecurityContext UID。要使 Astra 控制中心能够保护您的应用程序并将应用程序移动到 OpenShift 中的其他集群或项目，您需要添加策略，使应用程序能够作为任何 UID 运行。例如，以下 OpenShift 命令行界面命令会为 WordPress 应用程序授予相应的策略。

```
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
```

步骤

1. 选择 * 应用程序 * 。
2. 执行以下操作之一：
   - 在 * 操作 * 列中选择所需应用程序的选项菜单。
   - 选择所需应用程序的名称，然后选择页面右上角的状态下拉列表。
3. 选择 * 克隆 * 。
4. 指定克隆的详细信息：
   - 输入名称。
   - 选择克隆的目标集群。
   - 输入克隆的目标命名空间。与应用程序关联的每个源命名空间都会映射到您定义的目标命名空间。

     在克隆操作中、Astra Control会创建新的目标命名空间。指定的目标命名空间不能已存在于目标集群上。

   - 选择 * 下一步 * 。
   - 选择是要从现有快照还是备份创建克隆。如果不选择此选项，则 Astra 控制中心将根据应用程序的当前状态创建克隆。
     - 如果选择从现有快照或备份克隆、请选择要使用的快照或备份。
   - 选择 * 下一步 * 。
   - 选择将原始存储类与应用程序保持关联、或者选择其他存储类。

     您可以将应用程序的存储类迁移到本机云提供商存储类或其他受支持的存储类、 存储类 `ontap-nas` 在同一集群上、或者将应用程序复制到存储类由支持的另一集群 `ontap-nas-economy` 驱动程序。

   如果您选择了其他存储类、但在还原时此存储类不存在、则会返回错误。

5. 选择 * 下一步 * 。
6. 查看有关克隆的信息、然后选择*克隆*。

结果

Astra Control会根据您提供的信息克隆应用程序。当新应用程序克隆处于中时、克隆操作成功 `Healthy` 状态。

通过克隆或还原操作创建新命名空间后，帐户管理员 / 所有者可以编辑成员用户帐户并更新受影响用户的角色约束，以授予对新命名空间的访问权限。

> 在执行数据保护操作(克隆、备份或还原)并随后调整永久性卷大小后、在UI中显示新卷大小之前、最多会有20分钟的延迟。数据保护操作将在几分钟内成功完成，您可以使用存储后端的管理软件确认卷大小的更改。

管理应用程序执行挂钩

执行挂钩是一种自定义操作、您可以将其配置为与受管应用程序的数据保护操作结合运行。例如、如果您有一个数据库应用程序、则可以使用执行挂钩在快照之前暂停所有数据库事务、并在快照完成后恢复事务。这样可以确保应用程序一致的快照。

执行挂钩的类型

Astra Control支持以下类型的执行挂钩、具体取决于何时可以运行：

- 预快照
- 快照后
- 预备份
- 备份后
- 还原后

执行钩筛选器

在应用程序中添加或编辑执行连接时、您可以将筛选器添加到执行连接、以管理该连接将匹配的容器。对于在所有容器上使用相同容器映像的应用程序、筛选器非常有用、但可能会将每个映像用于不同的用途(例如Elasticsearch)。通过筛选器、您可以创建在某些相同容器上运行执行挂钩的情形、但不一定是所有容器上运行的情形。如果为单个执行钩创建多个筛选器、则这些筛选器将与逻辑运算符和运算符结合使用。每个执行连接最多可以有10个活动筛选器。

添加到执行挂钩中的每个筛选器都会使用一个正则表达式来匹配集群中的容器。当某个挂钩与某个容器匹配时、该挂钩将在该容器上运行其关联脚本。

> 筛选器的正则表达式使用正则表达式2 (RE2)语法、不支持创建从匹配列表中排除容器的筛选器。

有关Astra Control在执行挂钩筛选器中支持正则表达式语法的信息、请参见 "正则表达式2 (RE2)语法支持"。

有关自定义执行挂钩的重要注意事项

在为应用程序规划执行挂钩时，请考虑以下几点。

> 由于执行挂钩通常会减少或完全禁用其所运行的应用程序的功能，因此您应始终尽量缩短自定义执行挂钩运行所需的时间。
> 如果使用关联的执行挂钩启动备份或快照操作、但随后将其取消、则在备份或快照操作已开始时、仍允许运行这些挂钩。这意味着、备份后执行挂钩中使用的逻辑不能假定备份已完成。

- 执行挂钩必须使用脚本执行操作。许多执行挂钩可以引用同一个脚本。

- Astra Control要求执行挂钩使用的脚本以可执行Shell脚本的格式写入。
- 脚本大小限制为96 KB。
- Astra Control使用执行挂钩设置和任何匹配条件来确定哪些挂钩适用于快照、备份或还原操作。
- 所有执行挂钩故障均为软故障；即使某个挂钩发生故障、仍会尝试执行其他挂钩和数据保护操作。但是，如果挂机发生故障，则会在 * 活动 * 页面事件日志中记录一个警告事件。
- 要创建，编辑或删除执行挂钩，您必须是具有所有者，管理员或成员权限的用户。
- 如果执行挂机运行时间超过 25 分钟，则此挂机将失败，从而创建返回代码为不适用的事件日志条目。任何受影响的快照都将超时并标记为失败，并会生成一个事件日志条目，用于记录超时情况。
- 对于临时数据保护操作、所有挂机事件都会生成并保存在*活动*页面事件日志中。但是、对于计划的数据保护操作、事件日志中仅会记录挂钩故障事件(计划的数据保护操作本身生成的事件仍会记录下来)。
- 如果Astra Control Center将复制的源应用程序故障转移到目标应用程序、则在故障转移完成后、为源应用程序启用的任何还原后执行挂钩都会为目标应用程序运行。
- 如果将命名空间筛选器添加到在还原或克隆操作之后运行的执行挂钩、并且还原或克隆源和目标位于不同的命名空间中、则命名空间筛选器仅会应用于目标命名空间。

执行顺序

运行数据保护操作时、执行钩事件按以下顺序发生：

1. 任何适用的自定义操作前执行挂钩都会在相应的容器上运行。您可以根据需要创建和运行任意数量的自定义操作前挂钩、但操作前这些挂钩的执行顺序既不能保证也不可配置。
2. 执行数据保护操作。
3. 任何适用的自定义操作后执行挂钩都会在相应的容器上运行。您可以根据需要创建和运行任意数量的自定义操作后挂机、但这些挂机在操作后的执行顺序既不能保证也不可配置。

如果创建多个相同类型的执行挂钩(例如、预快照)、则无法保证这些挂钩的执行顺序。但是、可以保证不同类型的挂钩的执行顺序。例如、具有所有五种不同类型的挂钩的配置的执行顺序如下所示：

1. 已执行备份前的挂钩
2. 已执行预快照挂钩
3. 已执行后快照挂钩
4. 已执行备份后挂钩
5. 已执行还原后挂机

您可以从中的表中的第2种情形中查看此配置的示例 [确定挂钩是否会运行]。

> 在生产环境中启用执行钩脚本之前，应始终对其进行测试。您可以使用 "kubectl exec" 命令方便地测试脚本。在生产环境中启用执行挂钩后、请测试生成的快照和备份、以确保它们一致。为此、您可以将应用程序克隆到临时命名空间、还原快照或备份、然后测试应用程序。

确定挂钩是否会运行

使用下表帮助确定是否会为您的应用程序运行自定义执行挂钩。

请注意、所有高级应用程序操作都包括运行快照、备份或还原的基本操作之一。根据具体情况、克隆操作可能由

这些操作的各种组合组成、因此克隆操作运行时的执行挂钩将会有所不同。

原位还原操作需要现有快照或备份、因此这些操作不会运行快照或备份挂钩。

如果启动并取消包含快照的备份、并且存在关联的执行挂钩、则某些挂钩可能会运行、而其他挂钩则可能不会运行。这意味着、备份后执行挂钩不能假定备份已完成。对于已取消的备份以及关联的执行挂钩、请记住以下几点：

- 备份前和备份后的挂钩始终处于运行状态。
- 如果备份包含新快照且快照已启动、则会运行预快照和后快照挂钩。
- 如果在快照启动之前取消了备份、则不会运行预快照和后快照挂钩。

场景	操作	现有快照	现有备份	命名空间	集群	快照挂钩运行	备份挂钩运行	**Restore Hooks run**
1.	克隆	不包括	不包括	新增	相同	Y	不包括	Y
2.	克隆	不包括	不包括	新增	不同	Y	Y	Y
3.	克隆或还原	Y	不包括	新增	相同	不包括	不包括	Y
4.	克隆或还原	不包括	Y	新增	相同	不包括	不包括	Y
5.	克隆或还原	Y	不包括	新增	不同	不包括	不包括	Y
6.	克隆或还原	不包括	Y	新增	不同	不包括	不包括	Y
7.	还原	Y	不包括	现有	相同	不包括	不包括	Y
8.	还原	不包括	Y	现有	相同	不包括	不包括	Y
9.	Snapshot	不适用	不适用	不适用	不适用	Y	不适用	不适用
10.	备份	不包括	不适用	不适用	不适用	Y	Y	不适用
11.	备份	Y	不适用	不适用	不适用	不包括	不包括	不适用

执行钩示例

请访问 "NetApp Verda GitHub项目" 为Apache Cassandra和Elasticsearch等常见应用程序下载真正的执行挂钩。您还可以查看示例并了解如何构建自己的自定义执行挂钩。

查看现有执行挂钩

您可以查看应用程序的现有自定义执行挂钩。

步骤

1. 转到 * 应用程序 * ，然后选择受管应用程序的名称。
2. 选择 * 执行挂钩 * 选项卡。

   您可以在显示的列表中查看所有已启用或已禁用的执行挂钩。您可以查看挂钩的状态、匹配的容器数量、创

建时间以及运行时间(操作前或操作后)。您可以选择 + 此挂机名称旁边的图标可展开要运行它的容器列表。要查看与此应用程序的执行挂钩相关的事件日志、请转到*活动*选项卡。

查看现有脚本

您可以查看已上传的现有脚本。您还可以在此页面上查看正在使用哪些脚本以及正在使用哪些挂钩。

步骤

1. 转到*帐户*。
2. 选择*脚本*选项卡。

   您可以在此页面上查看已上传的现有脚本列表。*使用者*列显示了使用每个脚本的执行挂钩。

添加脚本

每个执行挂钩都必须使用脚本执行操作。您可以添加一个或多个可供执行挂钩引用的脚本。许多执行挂钩可以引用同一个脚本；这样、您就可以通过仅更改一个脚本来更新多个执行挂钩。

步骤

1. 转到*帐户*。
2. 选择*脚本*选项卡。
3. 选择 * 添加 * 。
4. 执行以下操作之一：
   - 上传自定义脚本。
     i. 选择 * 上传文件 * 选项。
     ii. 浏览到文件并上传。
     iii. 为脚本指定一个唯一名称。
     iv. （可选）输入其他管理员应了解的有关该脚本的任何注释。
     v. 选择*保存脚本*。
   - 从剪贴板粘贴到自定义脚本中。
     i. 选择*粘贴或类型*选项。
     ii. 选择文本字段并将脚本文本粘贴到字段中。
     iii. 为脚本指定一个唯一名称。
     iv. （可选）输入其他管理员应了解的有关该脚本的任何注释。
5. 选择*保存脚本*。

结果

新脚本将显示在*脚本*选项卡的列表中。

删除脚本

如果不再需要某个脚本、并且任何执行挂钩都不使用该脚本、则可以将其从系统中删除。

步骤

1. 转到*帐户*。
2. 选择*脚本*选项卡。
3. 选择要删除的脚本、然后在*操作*列中选择菜单。
4. 选择 * 删除 * 。

> 如果该脚本与一个或多个执行挂钩关联、则*删除*操作将不可用。要删除此脚本、请先编辑关联的执行挂钩、然后将其与其他脚本关联。

创建自定义执行挂钩

您可以为应用程序创建自定义执行挂钩。请参见 [执行钩示例] 有关挂机示例。要创建执行挂钩，您需要拥有所有者，管理员或成员权限。

> 创建用作执行挂钩的自定义Shell脚本时、请务必在文件开头指定适当的Shell、除非您正在运行特定命令或提供可执行文件的完整路径。

步骤

1. 选择 * 应用程序 * ，然后选择受管应用程序的名称。
2. 选择 * 执行挂钩 * 选项卡。
3. 选择 * 添加 * 。
4. 在*挂机详细信息*区域中：
   a. 从*操作*下拉菜单中选择操作类型、以确定何时应运行挂钩。
   b. 输入此挂钩的唯一名称。
   c. （可选）输入执行期间传递到挂机的任何参数，在输入的每个参数之后按 Enter 键以记录每个参数。
5. (可选)在*挂机筛选器详细信息*区域中、您可以添加筛选器来控制执行挂机运行在哪些容器上：
   a. 选择*添加筛选器*。
   b. 在*挂机筛选器类型*列中、从下拉菜单中选择要筛选的属性。
   c. 在*正则表达式*列中、输入要用作筛选器的正则表达式。Astra Control使用 "正则表达式2 (RE2)正则表达式语法"。

      > 如果在正则表达式字段中按属性的确切名称(例如Pod名称)进行筛选、而没有其他文本、则会执行子字符串匹配。要匹配确切的名称以及仅匹配该名称、请使用精确的字符串匹配语法(例如、 `^exact_podname$`）。

   d. 要添加更多筛选器、请选择*添加筛选器*。

      > 一个执行钩的多个筛选器与一个逻辑运算符和运算符结合使用。每个执行连接最多可以有10个活动筛选器。

6. 完成后、选择*下一步*。
7. 在 * 脚本 * 区域中，执行以下操作之一：

- 添加新脚本。
  i. 选择 * 添加 * 。
  ii. 执行以下操作之一：
    - 上传自定义脚本。
      I. 选择 * 上传文件 * 选项。
      II. 浏览到文件并上传。
      III. 为脚本指定一个唯一名称。
      IV. （可选）输入其他管理员应了解的有关该脚本的任何注释。
      V. 选择*保存脚本*。
    - 从剪贴板粘贴到自定义脚本中。
      I. 选择*粘贴或类型*选项。
      II. 选择文本字段并将脚本文本粘贴到字段中。
      III. 为脚本指定一个唯一名称。
      IV. （可选）输入其他管理员应了解的有关该脚本的任何注释。
- 从列表中选择一个现有脚本。

  这将指示执行挂钩使用此脚本。

8. 选择 * 下一步 * 。
9. 查看执行钩配置。
10. 选择 * 添加 * 。

检查执行挂钩的状态

在快照、备份或还原操作运行完毕后、您可以检查在该操作中运行的执行挂钩的状态。您可以使用此状态信息来确定是要保持执行状态、修改执行状态还是删除执行状态。

步骤

1. 选择 * 应用程序 * ，然后选择受管应用程序的名称。
2. 选择*数据保护*选项卡。
3. 选择*快照*可查看正在运行的快照、选择*备份*可查看正在运行的备份。

   *挂机状态*显示操作完成后执行挂机运行的状态。有关详细信息、可以将鼠标悬停在状态上。例如、如果在快照期间发生执行挂机故障、则将鼠标悬停在该快照的挂机状态上可显示失败的执行挂机列表。要查看每次失败的原因、您可以查看左侧导航区域中的*活动*页面。

查看脚本使用情况

您可以在Astra Control Web UI中查看哪些执行挂钩使用特定脚本。

步骤

1. 选择 * 帐户 * 。
2. 选择*脚本*选项卡。

   脚本列表中的*使用者*列包含有关列表中每个脚本使用哪些挂钩的详细信息。

3. 在*使用者*列中选择您感兴趣的脚本的信息。

   此时将显示一个更详细的列表、其中包含正在使用此脚本的挂钩的名称以及这些挂钩配置为运行的操作类型。

编辑执行挂钩

如果要更改执行挂钩的属性、筛选器或所使用的脚本、您可以编辑该执行挂钩。要编辑执行挂钩、您需要拥有所有者、管理员或成员权限。

步骤

1. 选择 * 应用程序 * ，然后选择受管应用程序的名称。
2. 选择 * 执行挂钩 * 选项卡。
3. 在*操作*列中选择要编辑的挂钩的选项菜单。
4. 选择 * 编辑 * 。
5. 完成每个部分后、选择*下一步*进行所需的更改。
6. 选择 * 保存 * 。

禁用执行挂钩

如果要暂时阻止执行挂钩在应用程序快照之前或之后运行，可以禁用执行挂钩。要禁用执行挂钩，您需要拥有所有者，管理员或成员权限。

步骤

1. 选择 * 应用程序 * ，然后选择受管应用程序的名称。
2. 选择 * 执行挂钩 * 选项卡。
3. 在 * 操作 * 列中选择要禁用的挂机的选项菜单。
4. 选择 * 禁用 * 。

删除执行挂钩

如果您不再需要执行挂钩，则可以将其完全移除。要删除执行挂钩，您需要拥有所有者，管理员或成员权限。

步骤

1. 选择 * 应用程序 * ，然后选择受管应用程序的名称。
2. 选择 * 执行挂钩 * 选项卡。
3. 在 * 操作 * 列中选择要删除的挂机的选项菜单。
4. 选择 * 删除 * 。
5. 在显示的对话框中、键入"delete"进行确认。

6. 选择*是、删除执行钩*。

有关详细信息 ...

- "NetApp Verda GitHub项目"

监控应用程序和集群运行状况

查看应用程序和集群运行状况摘要

选择 * 信息板 * 可查看应用程序，集群，存储后端及其运行状况的高级视图。

这些数字或状态不仅仅是静态数字或状态，您可以逐层查看。例如，如果应用程序未得到完全保护，您可以将鼠标悬停在图标上以确定哪些应用程序未得到完全保护，这包括原因。

应用程序区块

"* 应用程序 * " 图块可帮助您确定以下内容：

- 您当前使用 Astra 管理的应用程序数量。
- 这些受管应用程序是否运行正常。
- 应用程序是否受到完全保护（如果有最新备份可用，则会对其进行保护）。
- 已发现但尚未管理的应用程序的数量。

  理想情况下，此数字为零，因为您可能会在发现应用程序后对其进行管理或忽略。然后，您将监控信息板上发现的应用程序的数量，以确定开发人员何时向集群添加新应用程序。

集群图块

"* 集群 * " 图块提供了有关使用 Astra 控制中心管理的集群运行状况的类似详细信息，您可以像使用应用程序一样深入查看以获取更多详细信息。

存储后端图块

"Storage Backends* " 图块提供的信息可帮助您确定存储后端的运行状况，其中包括：

- 管理的存储后端数量
- 这些受管后端是否运行正常
- 后端是否受到完全保护
- 已发现但尚未管理的后端数量。

查看集群运行状况并管理存储类

添加要由 Astra 控制中心管理的集群后，您可以查看有关集群的详细信息，例如集群的位置，工作节点，永久性卷和存储类。您还可以更改受管集群的默认存储类。

查看集群运行状况和详细信息

您可以查看有关集群的详细信息、例如集群的位置、工作节点、永久性卷和存储类。

步骤

1. 在 Astra 控制中心 UI 中，选择 * 集群 * 。
2. 在 * 集群 * 页面上，选择要查看其详细信息的集群。

> 如果集群位于中 `removed` 状态虽然集群和网络连接运行状况良好(外部尝试使用Kubernetes API访问集群成功)、但您提供给Astra Control的kubeconfig可能不再有效。这可能是由于集群上的证书轮换或到期造成的。要更正此问题描述，请使用在 Astra Control 中更新与集群关联的凭据 "Astra Control API"。

3. 查看 * 概述 * ， * 存储 * 和 * 活动 * 选项卡上的信息，找到您要查找的信息。
   - * 概述 * ： 有关工作节点的详细信息，包括其状态。
   - * 存储 * ： 与计算关联的永久性卷，包括存储类和状态。
   - * 活动 * ： 显示与集群相关的活动。

> 您还可以从 Astra 控制中心 * 信息板 * 开始查看集群信息。在 * 资源摘要 * 下的 * 集群 * 选项卡上，您可以选择受管集群，此操作将转到 * 集群 * 页面。进入 * 集群 * 页面后，请按照上述步骤进行操作。

更改默认存储类

您可以更改集群的默认存储类。当Astra Control管理集群时、它会跟踪集群的默认存储类。

> 请勿使用kubectl命令更改存储类。请改用此操作步骤。如果使用kubectl进行更改、则Astra Control将还原这些更改。

步骤

1. 在Astra控制中心Web UI中、选择*集群*。
2. 在*集群*页面上、选择要更改的集群。
3. 选择 * 存储 * 选项卡。
4. 选择*存储类*类别。
5. 选择要设置为默认值的存储类的*操作*菜单。
6. 选择*设置为默认值*。

查看应用程序的运行状况和详细信息

开始管理某个应用程序后， Astra Control 会提供有关该应用程序的详细信息，使您能够确定其状态（是否运行正常），保护状态（是否在发生故障时受到全面保护）， Pod ，永久性存储等。

步骤

1. 在 Astra 控制中心 UI 中，选择 * 应用程序 * ，然后选择应用程序的名称。
2. 查看相关信息。
   - 应用程序状态：提供反映应用程序在Kubernetes中的状态的状态。例如， Pod 和永久性卷是否联机？如果某个应用程序运行状况不正常，您需要查看 Kubernetes 日志，对集群上的问题描述进行故障排除。Astra 不会提供任何信息来帮助您修复损坏的应用程序。
   - 应用程序保护状态：提供应用程序的保护程度状态：
     - * 完全保护 * ：应用程序具有一个活动备份计划，并且备份成功完成不到一周
     - * 部分保护 * ：应用程序具有活动备份计划，活动快照计划或成功备份或快照
     - * 未受保护 * ：既不受完全保护也不受部分保护的应用程序。

       You can't be Fully protected until you have a recent backup 。这一点非常重要，因为备份存储在对象存储中，而不是永久性卷。如果发生故障或意外事件会擦除集群及其永久性存储，则需要备份才能恢复。快照无法让您恢复。
   - 概述：有关与应用程序关联的Pod的状态的信息。
   - 数据保护：用于配置数据保护策略以及查看现有快照和备份。
   - 存储：显示应用程序级别的永久性卷。从 Kubernetes 集群的角度来看，永久性卷的状态。
   - 资源：用于验证正在备份和管理哪些资源。
   - 活动：显示与应用程序相关的活动。

> 您还可以从 Astra 控制中心 * 信息板 * 开始查看应用程序信息。在 * 资源摘要 * 下的 * 应用程序 * 选项卡上，您可以选择受管应用程序，此操作将转到 * 应用程序 * 页面。进入 * 应用程序 * 页面后，请按照上述步骤进行操作。

管理您的帐户

管理本地用户和角色

您可以使用Astra Control UI添加、删除和编辑Astra Control Center安装的用户。您可以使用 Astra Control UI 或 "Astra Control API" 以管理用户。

您还可以使用LDAP对选定用户执行身份验证。

使用 **LDAP**

LDAP是一种用于访问分布式目录信息的行业标准协议、也是企业身份验证的常见选择。您可以将Astra控制中心连接到LDAP服务器、以便对选定的Astra控制用户执行身份验证。从较高层面来看、该配置涉及将Astra与LDAP集成、并定义与LDAP定义对应的Astra Control用户和组。您可以使用Astra Control API或Web UI配置LDAP身份验证以及LDAP用户和组。有关详细信息、请参见以下文档：

- "使用Astra Control API管理远程身份验证和用户"
- "使用Astra Control UI管理远程用户和组"
- "使用Astra Control UI管理远程身份验证"

添加用户

帐户所有者和管理员可以向 Astra 控制中心安装添加更多用户。

步骤

1. 在 * 管理帐户 * 导航区域中，选择 * 帐户 * 。
2. 选择 * 用户 * 选项卡。
3. 选择 * 添加用户 * 。
4. 输入用户的名称，电子邮件地址和临时密码。

   用户需要在首次登录时更改密码。

5. 选择具有适当系统权限的用户角色。

   每个角色都提供以下权限：

   - * 查看器 * 可以查看资源。
   - " 成员 * " 具有 " 查看器 " 角色权限，可以管理应用程序和集群，取消管理应用程序以及删除快照和备份。
   - * 管理员 * 具有成员角色权限，可以添加和删除除所有者之外的任何其他用户。
   - * 所有者 * 具有管理员角色权限，可以添加和删除任何用户帐户。

6. 要为具有成员或查看器角色的用户添加约束，请启用 * 将角色限制为约束条件 * 复选框。

   有关添加约束的详细信息、请参见 "管理本地用户和角色"。

7. 选择 * 添加 * 。

管理密码

您可以在 Astra 控制中心管理用户帐户的密码。

更改密码

您可以随时更改用户帐户的密码。

步骤

1. 选择屏幕右上角的用户图标。
2. 选择 * 配置文件 * 。
3. 从选项菜单的 * 操作 * 列中选择 * 更改密码 * 。
4. 输入符合密码要求的密码。
5. 再次输入密码进行确认。
6. 选择 * 更改密码 * 。

重置其他用户的密码

如果您的帐户具有管理员或所有者角色权限，则可以重置其他用户帐户以及您自己的帐户的密码。重置密码时，

您需要分配一个临时密码，用户必须在登录时更改此密码。

步骤

1. 在 * 管理帐户 * 导航区域中，选择 * 帐户 * 。
2. 选择 * 操作 * 下拉列表。
3. 选择 * 重置密码 * 。
4. 输入符合密码要求的临时密码。
5. 再次输入密码进行确认。

   用户下次登录时，系统将提示用户更改密码。

6. 选择 * 重置密码 * 。

删除用户

具有所有者或管理员角色的用户可以随时从帐户中删除其他用户。

步骤

1. 在 * 管理帐户 * 导航区域中，选择 * 帐户 * 。
2. 在 * 用户 * 选项卡中，选中要删除的每个用户所在行中的复选框。
3. 从选项菜单的 * 操作 * 列中，选择 * 删除用户 / 秒 * 。
4. 出现提示时，键入单词 "remove" 并选择 * 是，删除用户 * 以确认删除。

结果

Astra 控制中心从帐户中删除用户。

管理角色

您可以通过添加命名空间限制并将用户角色限制为这些限制来管理角色。这样，您就可以控制对组织内资源的访问。您可以使用 Astra Control UI 或 "Astra Control API" 以管理角色。

向角色添加命名空间限制

管理员或所有者用户可以向成员或查看器角色添加命名空间限制。

步骤

1. 在 * 管理帐户 * 导航区域中，选择 * 帐户 * 。
2. 选择 * 用户 * 选项卡。
3. 在 * 操作 * 列中，为具有成员或查看器角色的用户选择菜单按钮。
4. 选择 * 编辑角色 * 。
5. 启用 * 将角色限制为约束条件 * 复选框。

   此复选框仅适用于 " 成员 " 或 " 查看器 " 角色。您可以从 * 角色 * 下拉列表中选择其他角色。

6. 选择 * 添加约束 * 。

您可以按命名空间或命名空间标签查看可用约束的列表。

7. 在 * 约束类型 * 下拉列表中，根据命名空间的配置方式选择 * Kubernetes 命名空间 * 或 * Kubernetes 命名空间标签 * 。
8. 从列表中选择一个或多个命名空间或标签，以构成一个限制，将角色限制为这些命名空间。
9. 选择 * 确认 * 。

   "* 编辑角色 * " 页面将显示您为此角色选择的约束列表。

10. 选择 * 确认 * 。

    在 * 帐户 * 页面上，您可以在 * 角色 * 列中查看任何成员或查看器角色的限制。

> 如果为某个角色启用了限制并选择了 * 确认 * 而未添加任何限制，则该角色将被视为具有完全限制（该角色将被拒绝访问分配给命名空间的任何资源）。

从角色中删除命名空间限制

管理员或所有者用户可以从角色中删除命名空间限制。

步骤

1. 在 * 管理帐户 * 导航区域中，选择 * 帐户 * 。
2. 选择 * 用户 * 选项卡。
3. 在 * 操作 * 列中，为具有成员或查看器角色且具有活动约束的用户选择菜单按钮。
4. 选择 * 编辑角色 * 。

   "* 编辑角色 " 对话框显示角色的活动约束。

5. 选择需要删除的约束右侧的 * X * 。
6. 选择 * 确认 * 。

有关详细信息 ...

- "用户角色和命名空间"

管理远程身份验证

LDAP是一种用于访问分布式目录信息的行业标准协议、也是企业身份验证的常见选择。您可以将Astra控制中心连接到LDAP服务器、以便对选定的Astra控制用户执行身份验证。

从较高层面来看、该配置涉及将Astra与LDAP集成、并定义与LDAP定义对应的Astra Control用户和组。您可以使用Astra Control API或Web UI配置LDAP身份验证以及LDAP用户和组。

> Astra控制中心使用ldap"mail"属性中的电子邮件地址搜索和跟踪远程用户。此属性可能是目录中的可选字段或空字段。对于要显示在Astra控制中心的任何远程用户、此字段中必须存在电子邮件地址。此电子邮件地址在Astra控制中心中用作用户名进行身份验证。

添加用于**LDAPS**身份验证的证书

为LDAP服务器添加专用TLS证书、以便在使用LDAPS连接时、Astra控制中心可以向LDAP服务器进行身份验证。您只需要执行一次此操作、或者在安装的证书过期时执行此操作。

步骤

1. 转到*帐户*。
2. 选择*证书*选项卡。
3. 选择 * 添加 * 。
4. 上传 `.pem` 将文件内容归档或粘贴到剪贴板中。
5. 选中*可信*复选框。
6. 选择*添加证书*。

启用远程身份验证

您可以启用LDAP身份验证并配置Astra Control与远程LDAP服务器之间的连接。

开始之前

如果您计划使用LDAPS、请确保将LDAP服务器的专用TLS证书安装在Astra控制中心中、以便Astra控制中心能够向LDAP服务器进行身份验证。请参见 添加用于LDAPS身份验证的证书 有关说明，请参见。

步骤

1. 转至*帐户>连接*。
2. 在*远程身份验证*窗格中、选择配置菜单。
3. 选择 * 连接 * 。
4. 输入服务器IP地址、端口和首选连接协议(LDAP或LDAPS)。

   作为最佳实践、请在与LDAP服务器连接时使用LDAPS。在连接到LDAPS之前、您需要在Astra控制中心安装LDAP服务器的专用TLS证书。

5. 以电子邮件格式输入服务帐户凭据(administrator@example.com)。在与LDAP服务器连接时、Astra Control将使用这些凭据。
6. 在*用户匹配*部分中、输入在从LDAP服务器检索用户信息时要使用的基础DN和相应的用户搜索筛选器。
7. 在*组匹配*部分中、输入组搜索基础DN和相应的自定义组搜索筛选器。

   请务必对*用户匹配*和*组匹配*使用正确的基本可分辨名称(DN)和适当的搜索筛选器。基础DN用于指示Astra Control在目录树的哪个级别开始搜索、而搜索筛选器用于限制目录树Astra Control搜索的各个部分。

8. 选择 * 提交 * 。

结果

与LDAP服务器建立连接后、远程身份验证*窗格状态将移至*待定、然后移至*已连接*。

禁用远程身份验证

您可以暂时禁用与LDAP服务器的活动连接。

> 禁用与LDAP服务器的连接时、将保存所有设置、并保留从该LDAP服务器添加到Astra Control中的所有远程用户和组。您可以随时重新连接到此LDAP服务器。

步骤

1. 转至*帐户>连接*。
2. 在*远程身份验证*窗格中、选择配置菜单。
3. 选择 * 禁用 * 。

结果

"远程身份验证"窗格状态将移至"*已禁用"。所有远程身份验证设置、远程用户和远程组都会保留下来、您可以随时重新启用连接。

编辑远程身份验证设置

如果禁用了与LDAP服务器的连接或*远程身份验证*窗格处于"连接错误"状态、则可以编辑配置设置。

> 如果*远程身份验证*窗格处于"已禁用"状态、则无法编辑LDAP服务器URL或IP地址。您需要 [断开远程身份验证] 第一个。

步骤

1. 转至*帐户>连接*。
2. 在*远程身份验证*窗格中、选择配置菜单。
3. 选择 * 编辑 * 。
4. 进行必要的更改、然后选择*编辑*。

断开远程身份验证

您可以从LDAP服务器断开连接、并从Astra Control中删除配置设置。

> 断开与LDAP服务器的连接后、该LDAP服务器的所有配置设置以及从该LDAP服务器添加的任何远程用户和组都会从Astra Control中删除。

步骤

1. 转至*帐户>连接*。
2. 在*远程身份验证*窗格中、选择配置菜单。
3. 选择*断开连接*。

结果

"远程身份验证"窗格状态将移至"*已断开连接"。远程身份验证设置、远程用户和远程组将从Astra Control中删除。

管理远程用户和组

如果您已在Astra Control系统上启用LDAP身份验证、则可以搜索LDAP用户和组、并将其包含在系统的已批准用户中。

添加远程用户

帐户所有者和管理员可以向Astra Control添加远程用户。

> 如果系统上已存在具有相同电子邮件地址的本地用户、则无法添加远程用户。要将此用户添加为远程用户、请先从系统中删除此本地用户。

> Astra控制中心使用ldap"mail"属性中的电子邮件地址搜索和跟踪远程用户。此属性可能是目录中的可选字段或空字段。对于要显示在Astra控制中心的任何远程用户、此字段中必须存在电子邮件地址。此电子邮件地址在Astra控制中心中用作用户名进行身份验证。

步骤

1. 转到*帐户*区域。
2. 选择*用户和组*选项卡。
3. 在页面最右侧、选择*远程用户*。
4. 选择 * 添加 * 。
5. 或者、也可以通过在*按电子邮件筛选*字段中输入用户的电子邮件地址来搜索LDAP用户。
6. 从列表中选择一个或多个用户。
7. 为用户分配角色。

   > 如果您为用户和用户组分配不同的角色、则优先使用较为宽松的角色。

8. (可选)为此用户分配一个或多个命名空间约束、然后选择*将角色限制为约束条件*以强制实施这些限制。您可以通过选择*添加约束*来添加新的命名空间约束。

   > 如果通过LDAP组成员资格为用户分配了多个角色、则只有最宽松角色中的限制才会生效。例如、如果具有本地查看器角色的用户加入了绑定到成员角色的三个组、则成员角色的约束之和将生效、而查看器角色的任何约束将被忽略。

9. 选择 * 添加 * 。

结果

新用户将显示在远程用户列表中。在此列表中、您可以查看用户的活动约束、并从*操作*菜单管理用户。

添加远程组

要一次性添加多个远程用户、帐户所有者和管理员可以向Astra Control添加远程组。添加远程组时、该组中的所有远程用户都会添加到Astra Control并继承相同的角色。

步骤

1. 转到*帐户*区域。
2. 选择*用户和组*选项卡。
3. 在页面最右侧、选择*远程组*。
4. 选择 * 添加 * 。

   在此窗口中、您可以看到Astra Control从目录中检索到的LDAP组的公用名和可分辨名称列表。

5. 或者、也可以在*按公用名筛选*字段中输入组的公用名来搜索LDAP组。
6. 从列表中选择一个或多个组。
7. 为组分配角色。

   您选择的角色将分配给此组中的所有用户。如果您为用户和用户组分配不同的角色、则优先使用较为宽松的角色。

8. (可选)为此组分配一个或多个命名空间约束、然后选择*将角色限制为约束条件*以强制实施这些限制。您可以通过选择*添加约束*来添加新的命名空间约束。

   如果通过LDAP组成员资格为用户分配了多个角色、则只有最宽松角色中的限制才会生效。例如、如果具有本地查看器角色的用户加入了绑定到成员角色的三个组、则成员角色的约束之和将生效、而查看器角色的任何约束将被忽略。

9. 选择 * 添加 * 。

结果

新组将显示在远程组列表中、而此组中的所有远程用户将显示在远程用户列表中。在此列表中、您可以查看有关该组的详细信息、并从*操作*菜单管理该组。

查看和管理通知

操作完成或失败时， Astra 会向您发出通知。例如，如果应用程序的备份成功完成，您将看到通知。

您可以从界面右上角管理这些通知：

步骤

1. 选择右上角的未读通知数量。
2. 查看通知，然后选择 * 标记为已读 * 或 * 显示所有通知 * 。

   如果选择 * 显示所有通知 * ，则会加载通知页面。

3. 在 * 通知 * 页面上，查看通知，选择要标记为已读的通知，选择 * 操作 * 并选择 * 标记为已读 * 。

添加和删除凭据

随时从您的帐户中添加和删除本地私有云提供商的凭据，例如 ONTAP S3 ，使用 OpenShift 管理的 Kubernetes 集群或非受管 Kubernetes 集群。Astra 控制中心使用这些凭据来发现 Kubernetes 集群和集群上的应用程序，并代表您配置资源。

请注意， Astra 控制中心中的所有用户都共享相同的凭据集。

添加凭据

您可以在管理集群时向 Astra 控制中心添加凭据。要通过添加新集群来添加凭据、请参见 "添加 Kubernetes 集群"。

> 创建自己的 `kubeconfig` file中、您只能定义*一*上下文元素。请参见 "Kubernetes 文档" 有关创建的信息 `kubeconfig` 文件。

删除凭据

随时从帐户中删除凭据。您只能在之后删除凭据 "取消管理所有关联集群"。

> 您添加到 Astra 控制中心的第一组凭据始终在使用中，因为 Astra 控制中心使用这些凭据向备份存储分段进行身份验证。最好不要删除这些凭据。

步骤

1. 选择 * 帐户 * 。
2. 选择 * 凭据 * 选项卡。
3. 在 * 状态 * 列中选择要删除的凭据的选项菜单。
4. 选择 * 删除 * 。
5. 键入单词 "remove" 确认删除，然后选择 * 是，删除凭据 * 。

结果

Astra 控制中心将从帐户中删除凭据。

监控帐户活动

您可以在 Astra Control 帐户中查看有关活动的详细信息。例如，邀请新用户时，添加集群时或创建快照时。您还可以将帐户活动导出到 CSV 文件。

> 如果您从Astra Control管理Kubernetes集群、并且Astra Control连接到Cloud Insights 、则Astra Control会将事件日志发送到Cloud Insights。日志信息(包括POD部署和PVC附件的相关信息)将显示在Astra Control Activity日志中。使用此信息确定您所管理的Kubernetes集群上的任何问题。

在 **Astra Control** 中查看所有帐户活动

1. 选择 * 活动 * 。
2. 使用筛选器缩小活动列表的范围，或者使用搜索框准确查找所需内容。

3. 选择 * 导出到 CSV* 将您的帐户活动下载到 CSV 文件。

查看特定应用程序的帐户活动

1. 选择 * 应用程序 * ，然后选择应用程序的名称。
2. 选择 * 活动 * 。

查看集群的帐户活动

1. 选择 * 集群 * ，然后选择集群的名称。
2. 选择 * 活动 * 。

采取措施解决需要关注的事件

1. 选择 * 活动 * 。
2. 选择需要关注的事件。
3. 选择 * 执行操作 * 下拉选项。

   从此列表中，您可以查看可能采取的更正操作，查看与问题描述 相关的文档，并获得支持以帮助解决问题描述 。

更新现有许可证

您可以将评估版许可证转换为完整许可证，也可以使用新许可证更新现有评估版许可证或完整许可证。如果您没有完整的许可证，请与 NetApp 销售联系人联系以获取完整的许可证和序列号。您可以使用Astra控制中心UI或 "Astra Control API" 更新现有许可证。

步骤

1. 登录到 "NetApp 支持站点"。
2. 访问 Astra 控制中心下载页面，输入序列号，然后下载完整的 NetApp 许可证文件（ NLF ）。
3. 登录到 Astra 控制中心 UI 。
4. 从左侧导航栏中，选择 * 帐户 * > * 许可证 * 。
5. 在 * 帐户 * > * 许可证 * 页面中，选择现有许可证的状态下拉菜单，然后选择 * 替换 * 。
6. 浏览到您下载的许可证文件。
7. 选择 * 添加 * 。
   - 帐户 * > * 许可证 * 页面显示许可证信息，到期日期，许可证序列号，帐户 ID 和使用的 CPU 单元。

有关详细信息 ...

- "Astra 控制中心许可"

管理存储分段

如果要备份应用程序和永久性存储，或者要跨集群克隆应用程序，则对象存储分段提供程序至关重要。使用 Astra 控制中心，添加一个对象存储提供程序作为应用程序的集群外备

份目标。

如果要将应用程序配置和永久性存储克隆到同一集群、则不需要存储分段。

使用以下 Amazon Simple Storage Service （ S3 ）存储分段提供商之一：

- NetApp ONTAP S3
- NetApp StorageGRID S3
- Microsoft Azure
- 通用 S3

Amazon Web Services (AWS)和Google Cloud Platform (GCP)使用通用S3存储分段类型。

虽然Astra控制中心支持将Amazon S3作为通用S3存储分段提供商、但Astra控制中心可能不支持声称支持Amazon S3的所有对象存储供应商。

存储分段可以处于以下状态之一：

- Pending ： 存储分段已计划进行发现。
- Available ： 存储分段可供使用。
- Removed：当前无法访问存储分段。

有关如何使用 Astra Control API 管理存储分段的说明，请参见 "Astra Automation 和 API 信息"。

您可以执行以下与管理存储分段相关的任务：

- "添加存储分段"
- [编辑存储分段]
- [设置默认分段]
- [轮换或删除存储分段凭据]
- [删除存储分段]

Astra 控制中心中的 S3 存储分段不会报告可用容量。在备份或克隆由 Astra 控制中心管理的应用程序之前，请检查 ONTAP 或 StorageGRID 管理系统中的存储分段信息。

编辑存储分段

您可以更改存储分段的访问凭据信息，并更改选定存储分段是否为默认存储分段。

添加存储分段时，请选择正确的存储分段提供程序，并为该提供程序提供正确的凭据。例如， UI 接受 NetApp ONTAP S3 作为类型并接受 StorageGRID 凭据；但是，这将发生原因使使用此存储分段执行所有未来应用程序备份和还原失败。请参见 "发行说明"。

步骤

1. 从左侧导航栏中、选择*分段*。

2. 从菜单的*操作*列中、选择*编辑*。
3. 更改存储分段类型以外的任何信息。

   您无法修改存储分段类型。

4. 选择 * 更新 * 。

设置默认分段

在集群间执行克隆时、Astra Control需要一个默认分段。按照以下步骤为所有集群设置默认存储分段。

步骤

1. 转至*云实例*。
2. 在列表中的*操作*列中为云实例选择菜单。
3. 选择 * 编辑 * 。
4. 在*分段*列表中、选择要用作默认分段的分段。
5. 选择 * 保存 * 。

轮换或删除存储分段凭据

Astra Control使用存储分段凭据获取访问权限、并为S3存储分段提供机密密钥、以便Astra控制中心可以与存储分段进行通信。

轮换存储分段凭据

如果要轮换凭据、请在维护窗口中没有正在进行的备份(计划备份或按需备份)时轮换凭据。

编辑和轮换凭据的步骤

1. 从左侧导航栏中、选择*分段*。
2. 从选项菜单的 * 操作 * 列中，选择 * 编辑 * 。
3. 创建新凭据。
4. 选择 * 更新 * 。

删除存储分段凭据

只有在已将新凭据应用于存储分段或存储分段不再处于活动状态时、才应删除存储分段凭据。

添加到 Astra Control 的第一组凭据始终处于使用状态，因为 Astra Control 使用这些凭据对备份存储分段进行身份验证。如果存储分段正在使用中、请勿删除这些凭据、因为这会导致备份失败和备份不可用。

如果删除了活动存储分段凭据、请参见 "对删除存储分段凭据进行故障排除"。

有关如何使用Astra Control API删除S3凭据的说明、请参见 "Astra Automation 和 API 信息"。

删除存储分段

您可以删除不再使用或运行状况不佳的存储分段。您可能需要执行此操作以使对象存储配置简单且最新。

> 您不能删除默认存储分段。如果要删除此存储分段，请先选择另一个存储分段作为默认存储。

开始之前

- 开始之前，应检查以确保此存储分段没有正在运行或已完成的备份。
- 您应进行检查，以确保存储分段未在任何活动保护策略中使用。

如果存在，您将无法继续。

步骤

1. 从左侧导航栏中，选择 * 分段器 * 。
2. 从 * 操作 * 菜单中，选择 * 删除 * 。

> Astra Control 可首先确保没有使用存储分段进行备份的计划策略，并且要删除的存储分段中没有活动备份。

3. 键入 "remove" 确认此操作。
4. 选择 * 是，删除存储分段 * 。

了解更多信息

- "使用 Astra Control API"

管理存储后端

通过将 Astra Control 中的存储集群作为存储后端进行管理，您可以在永久性卷（ PV ）和存储后端之间建立链接，并获得其他存储指标。您可以监控存储容量和运行状况详细信息，包括当 Astra 控制中心连接到 Cloud Insights 时的性能。

有关如何使用 Astra Control API 管理存储后端的说明，请参见 "Astra Automation 和 API 信息"。

您可以完成以下与管理存储后端相关的任务：

- "添加存储后端"
- [查看存储后端详细信息]
- [编辑存储后端身份验证详细信息]
- [管理已发现的存储后端]
- [取消管理存储后端]
- [删除存储后端]

查看存储后端详细信息

您可以从信息板或后端选项查看存储后端信息。

从信息板查看存储后端详细信息

步骤

1. 从左侧导航栏中选择 * 信息板 * 。
2. 查看信息板中显示状态的存储后端面板：
   - * 运行状况不正常 * ： 存储未处于最佳状态。这可能是由于延迟问题描述或应用程序因容器问题描述等原因而降级。
   - * 所有运行状况均正常 * ： 存储已进行管理并处于最佳状态。
   - * 已发现 * ： 存储已被发现，但未由 Astra Control 管理。

从后端选项查看存储后端详细信息

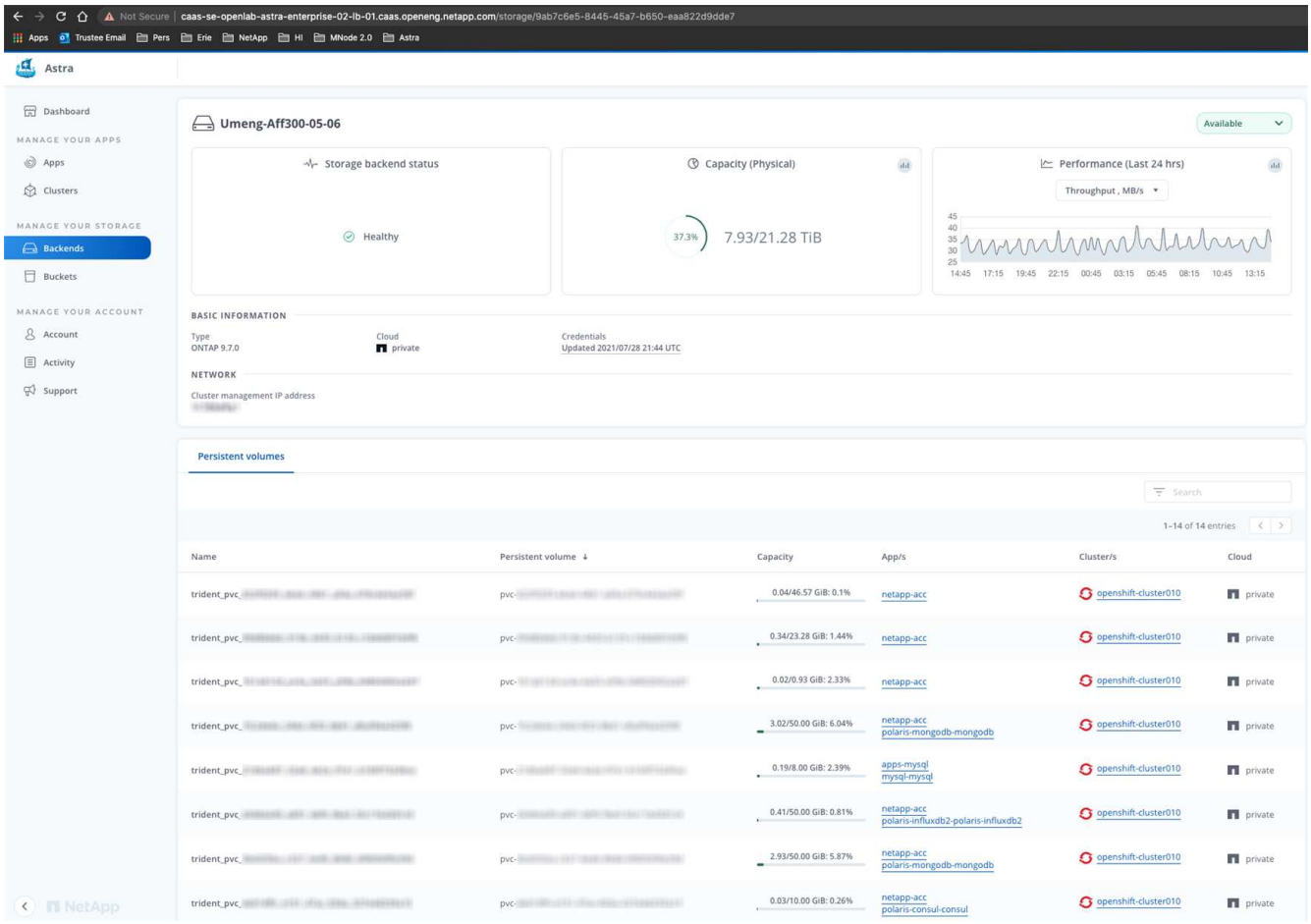
查看有关后端运行状况，容量和性能（ IOPS 吞吐量和 / 或延迟）的信息。

您可以查看Kubernetes应用程序正在使用的卷、这些卷存储在选定的存储后端。使用Cloud Insights 、您可以看到追加信息。请参见 "Cloud Insights 文档"。

步骤

1. 在左侧导航区域中，选择 * 后端 * 。
2. 选择存储后端。

如果您连接到 NetApp Cloud Insights ，则 Cloud Insights 中的数据摘录将显示在后端页面上。



3. 要直接转到 Cloud Insights ，请选择指标图像旁边的 * Cloud Insights * 图标。

编辑存储后端身份验证详细信息

Astra控制中心提供了两种对ONTAP 后端进行身份验证的模式。

- 基于凭据的身份验证：具有所需权限的ONTAP 用户的用户名和密码。您应使用预定义的安全登录角色(如admin)、以确保与ONTAP 版本的最大兼容性。
- 基于证书的身份验证：Astra控制中心还可以使用后端安装的证书与ONTAP 集群进行通信。您应使用客户端证书、密钥和可信CA证书(如果使用)(建议)。

您可以更新现有后端、以便从一种身份验证类型迁移到另一种身份验证方法。一次仅支持一种身份验证方法。

有关启用基于证书的身份验证的详细信息、请参见 "在ONTAP 存储后端启用身份验证"。

步骤

1. 从左侧导航栏中，选择 * 后端 * 。
2. 选择存储后端。
3. 在“凭据”字段中，选择*Edit*图标。
4. 在编辑页面中、选择以下选项之一。
    - 使用管理员凭据：输入ONTAP 集群管理IP地址和管理员凭据。凭据必须是集群范围的凭据。

您在此处输入凭据的用户必须具有 `ontapi` 在ONTAP 集群上的ONTAP 系统管理器中启用用户登录访问方法。如果您计划使用SnapMirror复制、请应用具有"admin"角色的用户凭据、该角色具有访问方法 `ontapi` 和 `http`、在源和目标ONTAP 集群上。请参见 "管理ONTAP 文档中的用户帐户" 有关详细信息 …

- 使用证书：上传证书 `.pem` file、证书密钥 `.key` 文件、以及证书颁发机构文件(可选)。

5. 选择 * 保存 * 。

管理已发现的存储后端

您可以选择管理未受管理但已发现的存储后端。管理存储后端时、Astra Control会指示用于身份验证的证书是否已过期。

步骤

1. 从左侧导航栏中，选择 * 后端 * 。
2. 选择*已发现*选项。
3. 选择存储后端。
4. 从“选项”菜单的“操作”列中，选择“管理”。
5. 进行更改。
6. 选择 * 保存 * 。

取消管理存储后端

您可以取消管理后端。

步骤

1. 从左侧导航栏中，选择 * 后端 * 。
2. 选择存储后端。
3. 从选项菜单的 * 操作 * 列中，选择 * 取消管理 * 。
4. 键入 "unmanage" 确认此操作。
5. 选择 * 是，取消管理存储后端 * 。

删除存储后端

您可以删除不再使用的存储后端。您可能需要执行此操作，以使您的配置简单且最新。

开始之前

- 确保存储后端未受管。
- 确保存储后端没有与集群关联的任何卷。

步骤

1. 从左侧导航栏中，选择 * 后端 * 。
2. 如果管理后端，请取消管理它。

a. 选择 * 受管 * 。
b. 选择存储后端。
c. 从*Actions*选项中，选择*Unmanage*。
d. 键入 "unmanage" 确认此操作。
e. 选择 * 是，取消管理存储后端 * 。

3. 选择 * 已发现 * 。
a. 选择存储后端。
b. 从*Actions*选项中，选择*Remove*。
c. 键入 "remove" 确认此操作。
d. 选择 * 是，删除存储后端 * 。

了解更多信息

- "使用 Astra Control API"

监控正在运行的任务

您可以在Astra Control中查看有关过去24小时内已完成、失败或已取消的正在运行的任务和任务的详细信息。例如、您可以查看正在运行的备份、还原或克隆操作的状态、并查看完成百分比和估计剩余时间等详细信息。您可以查看已运行的已计划操作或手动启动的操作的状态。

查看正在运行或已完成的任务时、您可以展开任务详细信息以查看每个子任务的状态。对于正在进行的或已完成的任务、任务进度条为绿色、对于已取消的任务、任务进度条为蓝色、对于因错误而失败的任务、任务进度条为红色。

对于克隆操作、任务子任务由快照和快照还原操作组成。

要查看有关失败任务的详细信息、请参见 "监控帐户活动"。

步骤

1. 在任务运行期间、转到*应用程序*。
2. 从列表中选择应用程序的名称。
3. 在应用程序的详细信息中、选择*任务*选项卡。

   您可以查看当前或过去任务的详细信息、并按任务状态进行筛选。

任务将在*任务*列表中保留长达24小时。您可以使用配置此限制以及其他任务监控器设置 "Astra Control API"。

使用Cloud Insights 、Prometheus或Fluentd连接监控基础架构

您可以配置多种可选设置来增强您的 Astra 控制中心体验。要监控和深入了解整个基础架构、请创建与NetApp Cloud Insights 的连接、配置Prometheus或添加Fluentd连接。

如果运行Astra控制中心的网络需要一个代理来连接到Internet (将支持包上传到NetApp 支持站点 或建立与Cloud Insights 的连接)、则应在Astra控制中心中配置一个代理服务器。

- 连接到 Cloud Insights
- 连接到Prometheus
- 连接到 Fluentd

添加一个代理服务器、用于连接到Cloud Insights 或NetApp 支持站点

如果运行Astra控制中心的网络需要一个代理来连接到Internet (将支持包上传到NetApp 支持站点 或建立与Cloud Insights 的连接)、则应在Astra控制中心中配置一个代理服务器。

Astra 控制中心不会验证您为代理服务器输入的详细信息。请确保输入正确的值。

步骤

1. 使用具有 * 管理员 / 所有者 * 权限的帐户登录到 Astra 控制中心。
2. 选择 * 帐户 * > * 连接 * 。
3. 从下拉列表中选择 * 连接 * 以添加代理服务器。

4. 输入代理服务器名称或 IP 地址以及代理端口号。
5. 如果代理服务器需要身份验证，请选中此复选框，然后输入用户名和密码。
6. 选择 * 连接 * 。

结果

如果您输入的代理信息已保存，则 * 帐户 * > * 连接 * 页面的 * HTTP 代理 * 部分将指示它已连接，并显示服务器名称。

编辑代理服务器设置

您可以编辑代理服务器设置。

步骤

1. 使用具有 * 管理员 / 所有者 * 权限的帐户登录到 Astra 控制中心。
2. 选择 * 帐户 * > * 连接 * 。
3. 从下拉列表中选择*Edit*以编辑连接。
4. 编辑服务器详细信息和身份验证信息。
5. 选择 * 保存 * 。

禁用代理服务器连接

您可以禁用代理服务器连接。在禁用之前，系统会警告您可能会对其他连接造成中断。

步骤

1. 使用具有 * 管理员 / 所有者 * 权限的帐户登录到 Astra 控制中心。
2. 选择 * 帐户 * > * 连接 * 。
3. 从下拉列表中选择 * 断开连接 * 以禁用连接。
4. 在打开的对话框中，确认操作。

连接到 Cloud Insights

要监控和深入了解整个基础架构，请将 NetApp Cloud Insights 与您的 Astra 控制中心实例连接起来。Cloud Insights 包含在您的 Astra 控制中心许可证中。

Cloud Insights 应可从 Astra 控制中心使用的网络访问，也可通过代理服务器间接访问。

当 Astra 控制中心连接到 Cloud Insights 时，将创建采集单元 POD 。此 POD 从由 Astra 控制中心管理的存储后端收集数据并将其推送到 Cloud Insights 。此 POD 需要 8 GB RAM 和 2 个 CPU 核。

当Astra控制中心与Cloud Insights 配对时，不应使用Cloud Insights 中的“*修改部署”选项。

启用Cloud Insights 连接后，您可以在*Backends*页面上查看吞吐量信息，并在选择存储后端后连接到Cloud Insights。您还可以在"Cluster"(集群)部分的*Dashboard (仪表板)*中找到相关信息，并从此处连接到Cloud Insights。

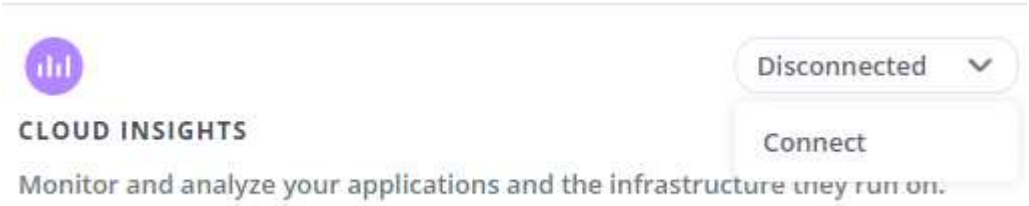
开始之前

- 具有 * 管理 / 所有者 * 权限的 Astra 控制中心帐户。
- 有效的 Astra Control Center 许可证。
- 如果运行 Astra 控制中心的网络需要使用代理连接到 Internet ，则为代理服务器。

如果您是 Cloud Insights 的新用户，请熟悉其特性和功能。请参见 "Cloud Insights 文档"。

步骤

1. 使用具有 * 管理员 / 所有者 * 权限的帐户登录到 Astra 控制中心。
2. 选择 * 帐户 * > * 连接 * 。
3. 选择 * 连接 * ，其中下拉列表中显示 * 已断开连接 * 以添加连接。



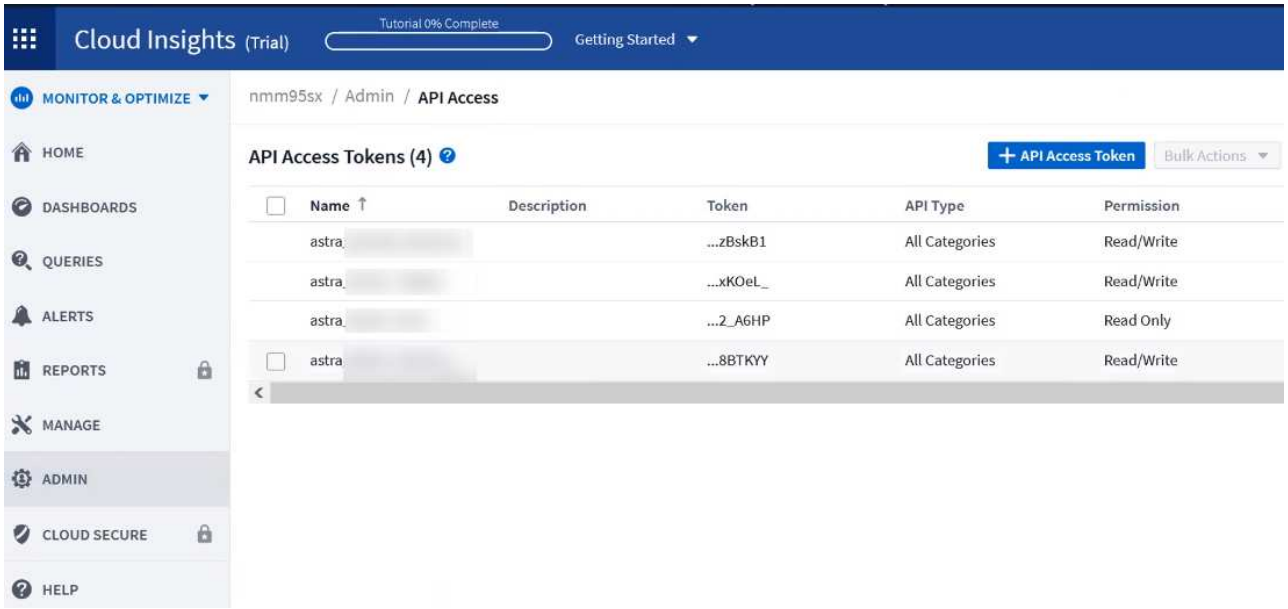
4. 输入 Cloud Insights API 令牌和租户 URL 。例如，租户 URL 采用以下格式：

```
https://<environment-name>.c01.cloudinsights.netapp.com/
```

获取 Cloud Insights 许可证后，您将获得租户 URL 。如果您没有租户 URL ，请参见 "Cloud Insights 文档"。

a. 以获取 "API 令牌"，登录到您的 Cloud Insights 租户 URL 。

b. 在 Cloud Insights 中，单击 * 管理 * > * API 访问 * 以生成 * 读 / 写 * 和 * 只读 * API 访问令牌。



c. 复制 * 只读 * 密钥。您需要将其粘贴到 Astra 控制中心窗口中以启用 Cloud Insights 连接。对于读取 API 访问令牌密钥权限，请选择：资产，警报，采集单元和数据收集。

d. 复制 * 读 / 写 * 密钥。您需要将其粘贴到 Astra 控制中心 * 连接 Cloud Insights * 窗口中。对于读/写API访问令牌密钥权限、请选择：数据载入、日志载入、采集单元和数据收集。

> 建议您生成 * 只读 * 密钥和 * 读 / 写 * 密钥，不要将同一密钥用于这两种用途。默认情况下，令牌到期期限设置为一年。我们建议您保留默认选择，以便为令牌提供到期前的最长持续时间。如果令牌过期，遥测将停止。

e. 将从 Cloud Insights 复制的密钥粘贴到 Astra 控制中心。

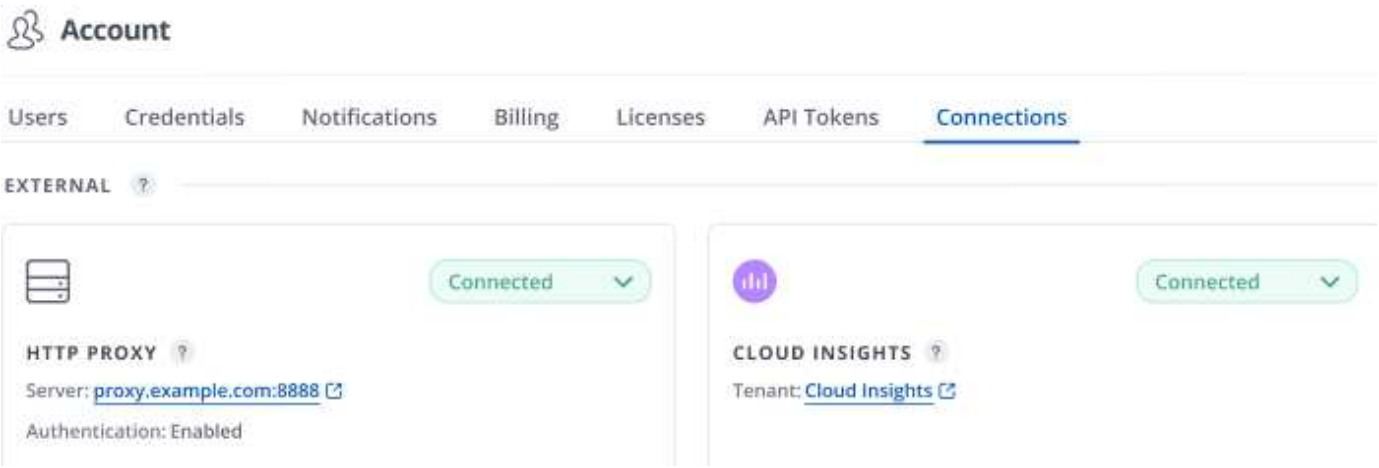
5. 选择 * 连接 * 。

> 选择 * 连接后，在 Cloud Insights * 帐户 * > * 连接 * 页面的 * 连接 * 部分中，连接状态将更改为 * 待定 * 。可以在几分钟内启用连接并将状态更改为 * 已连接 * 。

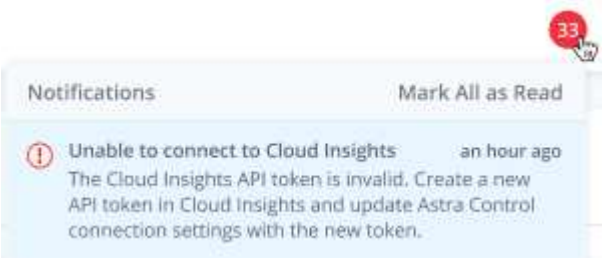
> 要在 Astra 控制中心和 Cloud Insights UI 之间轻松来回切换，请确保您已登录这两个。

在 **Cloud Insights** 中查看数据

如果连接成功，则 * 帐户 * > * 连接 * 页面的 * Cloud Insights * 部分将指示已连接，并显示租户 URL 。您可以访问 Cloud Insights 以查看成功接收和显示的数据。



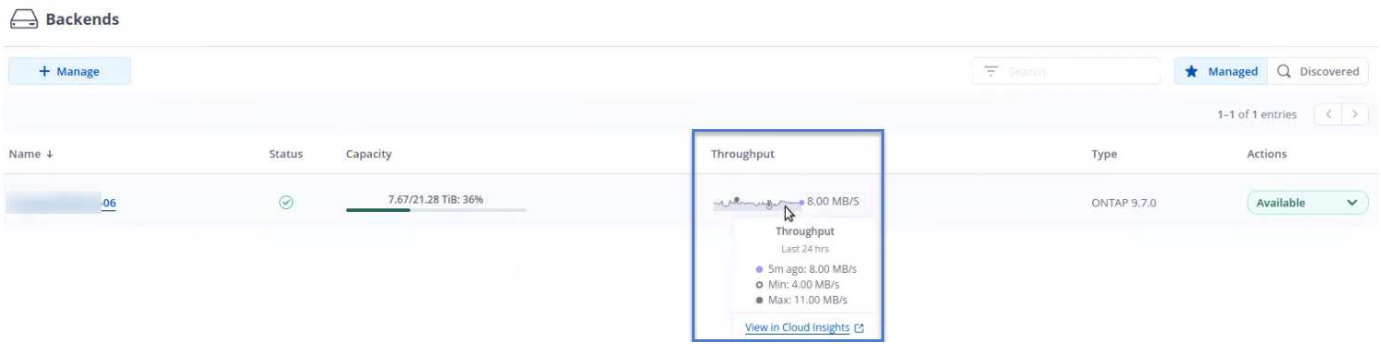
如果连接因某种原因失败，则状态将显示 * 失败 * 。您可以在用户界面右上角的 * 通知 * 下找到失败的原因。



您还可以在 * 帐户 * > * 通知 * 下找到相同的信息。

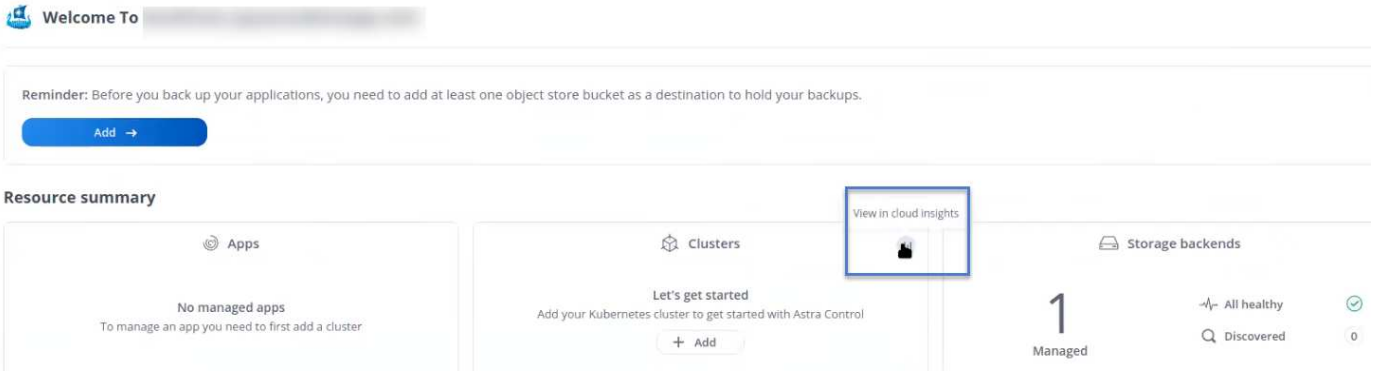
在 Astra 控制中心中，您可以在 * 后端 * 页面上查看吞吐量信息，并在选择存储后端后从此处连接到 Cloud

Insights 。



要直接转到 Cloud Insights ，请选择指标图像旁边的 * Cloud Insights * 图标。

您还可以在 * 信息板 * 上找到相关信息。



启用 Cloud Insights 连接后，如果删除在 Astra 控制中心添加的后端，后端将停止向 Cloud Insights 报告。

编辑 **Cloud Insights** 连接

您可以编辑 Cloud Insights 连接。

您只能编辑 API 密钥。要更改 Cloud Insights 租户 URL ，我们建议您断开 Cloud Insights 连接并使用新 URL 进行连接。

步骤

1. 使用具有 * 管理员 / 所有者 * 权限的帐户登录到 Astra 控制中心。
2. 选择 * 帐户 * > * 连接 * 。
3. 从下拉列表中选择*Edit*以编辑连接。
4. 编辑 Cloud Insights 连接设置。
5. 选择 * 保存 * 。

禁用 **Cloud Insights** 连接

您可以为由 Astra 控制中心管理的 Kubernetes 集群禁用 Cloud Insights 连接。禁用 Cloud Insights 连接不会删除已上传到 Cloud Insights 的遥测数据。

步骤

1. 使用具有 * 管理员 / 所有者 * 权限的帐户登录到 Astra 控制中心。
2. 选择 * 帐户 * > * 连接 * 。
3. 从下拉列表中选择 * 断开连接 * 以禁用连接。
4. 在打开的对话框中，确认操作。
   确认此操作后，在 * 帐户 * > * 连接 * 页面上， Cloud Insights 状态将更改为 * 待定 * 。要将状态更改为 * 已断开连接 * ，需要几分钟的时间。

连接到Prometheus

您可以使用Prometheus监控Astra控制中心数据。您可以将Prometheus配置为从Kubernetes集群指标端点收集指标、也可以使用Prometheus可视化指标数据。

有关使用Prometheus的详细信息、请参见其文档、网址为 "Prometheus入门"。

您将需要什么

确保已在Astra控制中心集群或可与Astra控制中心集群通信的其他集群上下载并安装Prometheus软件包。

按照官方文档中的说明进行操作 "安装 Prometheus"。

Prometheus需要能够与Astra控制中心Kubernetes集群进行通信。如果Astra控制中心集群上未安装Prometheus、您需要确保这些模块能够与Astra控制中心集群上运行的指标服务进行通信。

配置 Prometheus

Astra控制中心会在Kubernetes集群中的TCP端口9090上公开指标服务。您需要配置 Prometheus 以从此服务收集指标。

步骤

1. 登录到Prometheus服务器。
2. 将集群条目添加到中 `prometheus.yml` 文件在中 `yml` 文件中、为集群添加一个类似于以下内容的条目 `scrape_configs section`：

```
job_name: '<Add your cluster name here. You can abbreviate. It just
needs to be a unique name>'
  metrics_path: /accounts/<replace with your account ID>/metrics
  authorization:
     credentials: <replace with your API token>
  tls_config:
     insecure_skip_verify: true
  static_configs:
    - targets: ['<replace with your astraAddress. If using FQDN, the
prometheus server has to be able to resolve it>']
```

如果您设置了 `tls_config insecure_skip_verify` to `true`、不需要TLS加密协议。

3. 重新启动Prometheus服务：

```
sudo systemctl restart prometheus
```

访问**Prometheus**

访问Prometheus URL。

步骤

1. 在浏览器中、输入端口为9090的Prometheus URL。
2. 选择*状态*>*目标*以验证您的连接。

在**Prometheus**中查看数据

您可以使用Prometheus查看Astra控制中心数据。

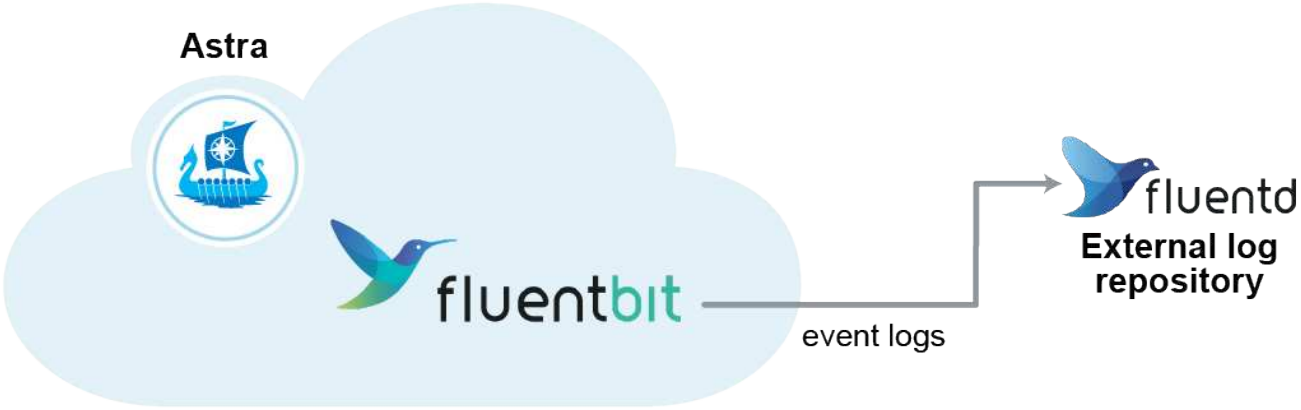
步骤

1. 在浏览器中、输入Prometheus URL。
2. 从Prometheus菜单中、选择*图形*。
3. 要使用指标资源管理器、请选择*执行*旁边的图标。
4. 选择 … `scrape_samples_scraped` 并选择*执行*。
5. 要查看随时间推移的样本擦除了、请选择*图形*。

如果收集了多个集群数据、则每个集群的指标将以不同的颜色显示。

连接到 **Fluentd**

您可以将日志(Kubennet事件)从Astra Control Center监控的系统发送到Fluentd端点。默认情况下， Fluentd 连接处于禁用状态。



只有受管集群中的事件日志才会转发到 Fluentd 。

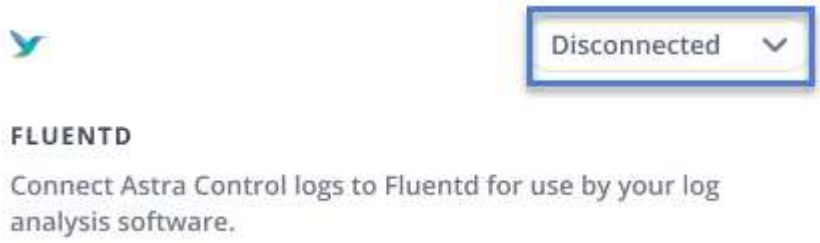
开始之前

- 具有 * 管理 / 所有者 * 权限的 Astra 控制中心帐户。
- 已在 Kubernetes 集群上安装并运行 Astra Control Center 。

Astra 控制中心不会验证您为 Fluentd 服务器输入的详细信息。请确保输入正确的值。

步骤

1. 使用具有 * 管理员 / 所有者 * 权限的帐户登录到 Astra 控制中心。
2. 选择 * 帐户 * > * 连接 * 。
3. 从显示 * 已断开连接 * 的下拉列表中选择 * 连接 * 以添加连接。



4. 输入 Fluentd 服务器的主机 IP 地址，端口号和共享密钥。
5. 选择 * 连接 * 。

结果

如果您为 Fluentd 服务器输入的详细信息已保存，则 * 帐户 * > * 连接 * 页面的 * 通量 * 部分将指示它已连接。现在，您可以访问已连接的 Fluentd 服务器并查看事件日志。

如果连接因某种原因失败，则状态将显示 * 失败 * 。您可以在用户界面右上角的 * 通知 * 下找到失败的原因。

您还可以在 * 帐户 * > * 通知 * 下找到相同的信息。

如果您在收集日志时遇到问题、应登录到工作节点并确保日志在中可用 `/var/log/containers/`。

编辑 **Fluentd** 连接

您可以编辑与 Astra Control Center 实例的 Fluentd 连接。

步骤

1. 使用具有 * 管理员 / 所有者 * 权限的帐户登录到 Astra 控制中心。
2. 选择 * 帐户 * > * 连接 * 。
3. 从下拉列表中选择*Edit*以编辑连接。
4. 更改 Fluentd 端点设置。

5. 选择 * 保存 * 。

禁用 **Fluentd** 连接

您可以禁用与 Astra Control Center 实例的 Fluentd 连接。

步骤

1. 使用具有 * 管理员 / 所有者 * 权限的帐户登录到 Astra 控制中心。
2. 选择 * 帐户 * > * 连接 * 。
3. 从下拉列表中选择 * 断开连接 * 以禁用连接。
4. 在打开的对话框中，确认操作。

取消管理应用程序和集群

从 Astra 控制中心删除不再需要管理的任何应用程序或集群。

取消管理应用程序

从 Astra 控制中心停止管理不再需要备份，快照或克隆的应用程序。

取消管理应用程序时：

- 所有现有备份和快照都将被删除。
- 应用程序和数据始终可用。

步骤

1. 从左侧导航栏中，选择 * 应用程序 * 。
2. 选择应用程序。
3. 从选项菜单的操作列中、选择*取消管理*。
4. 查看相关信息。
5. 键入 "unmanage" 进行确认。
6. 选择*是、取消管理应用程序*。

结果

Astra 控制中心停止管理应用程序。

取消管理集群

停止从Astra控制中心管理不再需要管理的集群。

在取消管理集群之前，您应取消管理与集群关联的应用程序。

取消管理集群时：

- 此操作将停止由 Astra 控制中心管理集群。它不会对集群的配置进行任何更改，也不会删除集群。
- 不会从集群中卸载 Astra Trident 。 "了解如何卸载 Astra Trident"。

步骤

1. 从左侧导航栏中，选择 * 集群 * 。
2. 选中不再要管理的集群对应的复选框。
3. 从选项菜单的 * 操作 * 列中，选择 * 取消管理 * 。
4. 确认要取消管理集群，然后选择 * 是，取消管理集群 * 。

结果

集群状态将更改为*正在删除*。之后、集群将从*集群*页面中删除、不再由Astra控制中心管理。

如果 Astra 控制中心和 Cloud Insights 未连接 * ，则取消管理集群将删除为发送遥测数据而安装的所有资源。如果已连接Astra控制中心和Cloud Insights *、则取消管理集群将仅删除 `fluentbit` 和 `event-exporter` POD。

升级 Astra 控制中心

要升级Astra控制中心、请从NetApp 支持站点 下载安装包并完成以下说明。您可以使用此操作步骤在互联网连接或通风环境中升级 Astra 控制中心。

开始之前

- 升级之前、请参见 "操作环境要求" 确保您的环境仍满足Astra Control Center部署的最低要求。您的环境应具有以下内容：
  - 受支持的Astra三项功能版本
    要确定您正在运行的版本、请对现有Astra Control Center运行以下命令：

    ```
    kubectl get tridentversion -n trident
    ```

    请参见 "Astra Trident 文档" 从旧版本升级。

    要升级到Kubernetes 1.25、您必须升级到Astra Trident 22.10 先前版本。

  - 受支持的Kubbernetes分发版
    要确定您正在运行的版本、请对现有Astra Control Center运行以下命令： `kubectl get nodes -o wide`
  - 集群资源充足
    要确定集群资源、请在现有Asta Control Center集群中运行以下命令： `kubectl describe node <node name>`
  - 可用于推送和上传Astra控制中心映像的注册表
  - 默认存储类
    要确定默认存储类、请对现有Astra Control Center运行以下命令： `kubectl get storageclass`

- (仅限OpenShift)确保所有集群操作员均处于运行状况良好且可用。

```
kubectl get clusteroperators
```

- 确保所有 API 服务均处于运行状况良好且可用。

```
kubectl get apiservices
```

- 在开始升级之前、请从Astra控制中心用户界面中注销。

关于此任务

Astra 控制中心升级过程将指导您完成以下高级步骤：

- 下载并提取Astra控制中心
- 删除NetApp Astra kubectl插件并重新安装
- [将映像添加到本地注册表]
- 安装更新后的 Astra 控制中心操作员
- 升级 Astra 控制中心
- [验证系统状态]

请勿删除Astra Control Center运算符(例如、 `kubectl delete -f astra_control_center_operator_deploy.yaml`)、以避免删除Pod。

如果计划，备份和快照未运行，请在维护窗口中执行升级。

下载并提取**Astra**控制中心

1. 转至 "Astra Control Center产品下载页面" 页面。您可以从下拉菜单中选择所需的最新版本或其他版本。
2. 下载包含Astra Control Center的软件包 (`astra-control-center-[version].tar.gz`）。
3. (建议但可选)下载Astra控制中心的证书和签名包 (`astra-control-center-certs-[version].tar.gz`)以验证捆绑包的签名：

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

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

此时将显示输出 `Verified OK` 验证成功后。

4. 从Astra Control Center捆绑包中提取映像：

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

删除NetApp Astra kubectl插件并重新安装

您可以使用NetApp Asta kubect命令行插件将映像推送到本地Docker存储库。

1. 确定是否已安装此插件：

```
kubectl astra
```

2. 执行以下操作之一：
   - 如果已安装此插件、则此命令应返回kubectl插件帮助。要删除现有版本的kubectl-Astra、请运行以下命令： `delete /usr/local/bin/kubectl-astra`。
   - 如果此命令返回错误、则表示未安装此插件、您可以继续执行下一步以安装它。
3. 安装插件：
   a. 列出可用的NetApp Astra kubectl插件二进制文件、并记下操作系统和CPU架构所需的文件名称：

   kubectl插件库是tar包的一部分、并会解压缩到文件夹中 `kubectl-astra`。

```
ls kubectl-astra/
```

   a. 将正确的二进制文件移动到当前路径并重命名为 `kubectl-astra`：

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

将映像添加到本地注册表

1. 为容器引擎完成相应的步骤顺序：

Docker

1. 更改为tarball的根目录。您应看到此文件和目录：

   ```
   acc.manifest.bundle.yaml
   acc/
   ```

2. 将Astra Control Center映像目录中的软件包映像推送到本地注册表。在运行之前、请进行以下替换 `push-images` 命令：

   - 将<BUNDLE_FILE> 替换为Astra Control捆绑包文件的名称 (`acc.manifest.bundle.yaml`）。
   - 将<MY_FULL_REGISTRY_PATH> 替换为Docker存储库的URL；例如 "<a href="https://<docker-registry>"" class="bare">https://<docker-registry>"。
   - 将<MY_REGISTRY_USER> 替换为用户名。
   - 将<MY_REGISTRY_TOKEN> 替换为注册表的授权令牌。

     ```
     kubectl astra packages push-images -m <BUNDLE_FILE> -r
     <MY_FULL_REGISTRY_PATH> -u <MY_REGISTRY_USER> -p
     <MY_REGISTRY_TOKEN>
     ```

Podman

1. 更改为tarball的根目录。您应看到此文件和目录：

   ```
   acc.manifest.bundle.yaml
   acc/
   ```

2. 登录到注册表：

   ```
   podman login <YOUR_REGISTRY>
   ```

3. 准备并运行以下针对您使用的Podman版本自定义的脚本之一。将<MY_FULL_REGISTRY_PATH> 替换为包含任何子目录的存储库的URL。

   ```
   <strong>Podman 4</strong>
   ```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.04.2-7
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done
```

```
<strong>Podman 3</strong>
```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.04.2-7
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done
```

根据您的注册表配置、此脚本创建的映像路径应类似于以下内容：

```
https://netappdownloads.jfrog.io/docker-astra-control-
prod/netapp/astra/acc/23.04.2-7/image:version
```

安装更新后的 Astra 控制中心操作员

1. 更改目录：

```
cd manifests
```

2. 编辑Astra控制中心操作员部署YAML (`astra_control_center_operator_deploy.yaml`)以引用您的本地注册表和密钥。

```
vim astra_control_center_operator_deploy.yaml
```

a. 如果您使用的注册表需要身份验证、请替换或编辑的默认行 `imagePullSecrets: []` 使用以下命令：

```
imagePullSecrets: [{name: astra-registry-cred}]
```

b. 更改 `[your_registry_path]` 。 `kube-rbac-proxy` 将映像推送到注册表路径中 上一步。

c. 更改 `[your_registry_path]` 。 `acc-operator` 将映像推送到注册表路径中 上一步。

d. 将以下值添加到 `env` 部分。

```
- 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
  strategy:
    type: Recreate
  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
      env:
      - name: ACCOP_LOG_LEVEL
        value: "2"
      - name: ACCOP_HELM_UPGRADETIMEOUT
        value: 300m
      image: [your_registry_path]/acc-operator:23.04.36
      imagePullPolicy: IfNotPresent
      livenessProbe:
        httpGet:
          path: /healthz
          port: 8081
        initialDelaySeconds: 15
        periodSeconds: 20
      name: manager
      readinessProbe:
        httpGet:
          path: /readyz
          port: 8081
        initialDelaySeconds: 5
        periodSeconds: 10
      resources:
        limits:
          cpu: 300m
          memory: 750Mi
        requests:
          cpu: 100m
          memory: 75Mi
      securityContext:
        allowPrivilegeEscalation: false
    imagePullSecrets: []
    securityContext:
      runAsUser: 65532
    terminationGracePeriodSeconds: 10
```

3. 安装更新后的 Astra 控制中心操作员：

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

响应示例：

```
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. 验证Pod是否正在运行：

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

升级 **Astra** 控制中心

1. 编辑Astra Control Center自定义资源(CR)：

```
kubectl edit AstraControlCenter -n [netapp-acc or custom namespace]
```

2. 更改Astra版本号 (`astraVersion` 在中 `spec`)升级到要升级到的版本：

```
spec:
  accountName: "Example"
  astraVersion: "[Version number]"
```

3. 验证您的映像注册表路径是否与您在中将映像推送到的注册表路径匹配 上一步。更新 `imageRegistry` 在中 `spec` 注册表自上次安装以来是否发生了更改。

```
  imageRegistry:
    name: "[your_registry_path]"
```

4. 将以下内容添加到 `crds` 中的配置 `spec`：

```
crds:
  shouldUpgrade: true
```

5. 在中添加以下行 `additionalValues` 在中 `spec` 在Astra控制中心CR中：

```
additionalValues:
    nautilus:
      startupProbe:
        periodSeconds: 30
        failureThreshold: 600
```

6. 保存并退出文件编辑器。此时将应用所做的更改、并开始升级。
7. （可选）验证 Pod 是否终止并重新可用：

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

8. 等待Astra Control状态条件指示升级已完成且准备就绪 (`True`）：

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

响应：

```
NAME    UUID                                   VERSION     ADDRESS
READY
astra   9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f   23.04.2-7
10.111.111.111  True
```

要在操作期间监控升级状态、请运行以下命令： `kubectl get AstraControlCenter -o yaml -n [netapp-acc or custom namespace]`

要检查Astra控制中心操作员日志、请运行以下命令：
`kubectl logs deploy/acc-operator-controller-manager -n netapp-acc-operator -c manager -f`

验证系统状态

1. 登录到 Astra 控制中心。
2. 验证此版本是否已升级。请参见用户界面中的*支持*页面。
3. 验证所有受管集群和应用程序是否仍存在并受到保护。

卸载 Astra 控制中心

如果要从试用版升级到完整版本的产品，您可能需要删除 Astra Control Center 组件。要删除 Astra 控制中心和 Astra 控制中心操作员，请按顺序运行此操作步骤中所述的命令。

如果您在卸载时遇到任何问题，请参见 [对卸载问题进行故障排除]。

开始之前

1. "取消管理所有应用程序" 。
2. "取消管理所有集群"。

步骤

1. 删除 Astra 控制中心。以下命令示例基于默认安装。如果已进行自定义配置，请修改命令。

```
kubectl delete -f astra_control_center.yaml -n netapp-acc
```

结果

```
astracontrolcenter.astra.netapp.io "astra" deleted
```

2. 使用以下命令删除 `netapp-acc` (或自定义名称)命名空间：

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

结果示例：

```
namespace "netapp-acc" deleted
```

3. 使用以下命令删除 Astra 控制中心操作员系统组件：

```
kubectl delete -f astra_control_center_operator_deploy.yaml
```

结果

```
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
```

对卸载问题进行故障排除

使用以下解决方法解决卸载 Astra 控制中心时出现的任何问题。

卸载 **Astra** 控制中心无法清理受管集群上的监控操作员 **POD**

如果在卸载 Astra Control Center 之前未取消管理集群，则可以使用以下命令手动删除 netapp-monitoring 命名空间和命名空间中的 Pod：

步骤

1. 删除 `acc-monitoring` 代理：

```
kubectl delete agents acc-monitoring -n netapp-monitoring
```

结果

```
agent.monitoring.netapp.com "acc-monitoring" deleted
```

2. 删除命名空间：

```
kubectl delete ns netapp-monitoring
```

结果

```
namespace "netapp-monitoring" deleted
```

3. 确认已删除资源：

```
kubectl get pods -n netapp-monitoring
```

结果

```
No resources found in netapp-monitoring namespace.
```

4. 确认已删除监控代理：

```
kubectl get crd|grep agent
```

示例结果：

```
agents.monitoring.netapp.com                    2021-07-21T06:08:13Z
```

5. 删除自定义资源定义（ CRD ）信息：

```
kubectl delete crds agents.monitoring.netapp.com
```

结果

```
customresourcedefinition.apiextensions.k8s.io
"agents.monitoring.netapp.com" deleted
```

卸载 **Astra** 控制中心无法清理 **Traefik CRD**

您可以手动删除 Traefik CRD 。CRD 是全局资源，删除它们可能会影响集群上的其他应用程序。

步骤

1. 列出集群上安装的 Traefik CRD：

```
kubectl get crds |grep -E 'traefik'
```

响应

```
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. 删除 CRD：

```
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
```

了解更多信息

- "卸载的已知问题"