概念
Astra Control Center

NetApp
November 27, 2023

This PDF was generated from https://docs.netapp.com/zh-cn/astra-control-center-2307/concepts/architecture.html on November 27, 2023. Always check docs.netapp.com for the latest.

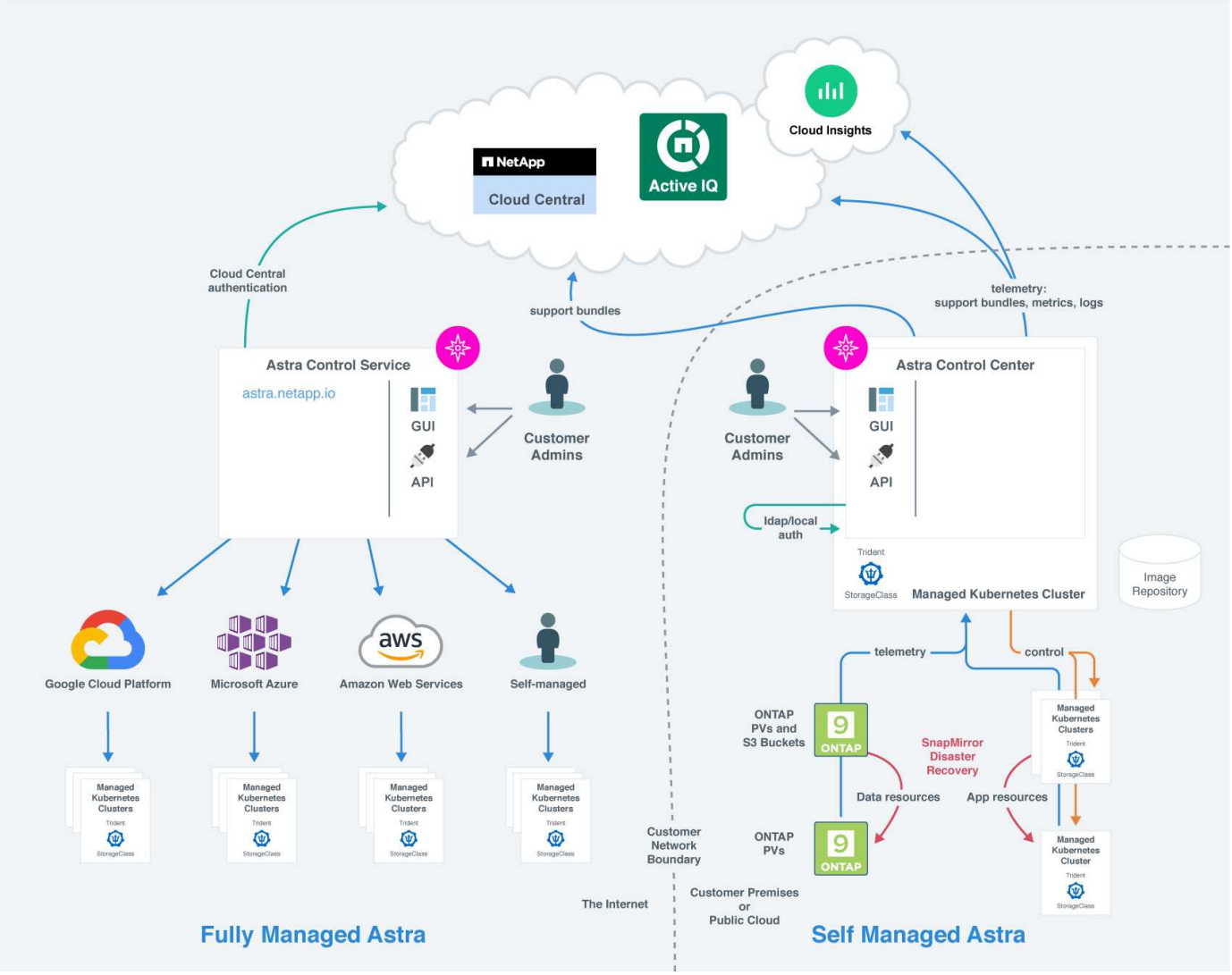
目录

概念 1
- 架构和组件 1
- 数据保护 2
- 许可 5
- 应用程序管理 6
- 存储类和永久性卷大小 8
- 用户角色和命名空间 9
- POD安全性 9

概念

架构和组件

下面简要介绍了 Astra Control 环境的各个组件。



Astra Control 组件

- * Kubernetes 集群 * ： Kubernetes 是一个可移植，可扩展的开源平台，用于管理容器化工作负载和服务，便于进行声明性配置和自动化。Astra 为 Kubernetes 集群中托管的应用程序提供管理服务。
- * Astra Trident * ：作为由 NetApp 维护的完全受支持的开源存储配置程序和编排程序， Astra Trident 使您能够为 Docker 和 Kubernetes 管理的容器化应用程序创建存储卷。使用Astra控制中心部署时、Astra Trident会包括一个已配置的ONTAP 存储后端。
- * 存储后端 * ：
  - Astra控制服务使用以下存储后端：
    - "适用于 Google Cloud 的 NetApp Cloud Volumes Service" 或Google Persistent Disk作为GKE集群

的存储后端

- "Azure NetApp Files" 或Azure受管磁盘作为AKS集群的存储后端。
- "Amazon Elastic Block Store (EBS)" 或 "适用于 NetApp ONTAP 的 Amazon FSX" 作为EKS集群的后端存储选项。

◦ Astra 控制中心使用以下存储后端：

- ONTAP AFF 、FAS 和ASA。作为存储软件和硬件平台， ONTAP 可提供核心存储服务，支持多个存储访问协议以及快照和镜像等存储管理功能。
- Cloud Volumes ONTAP

- **Astra**：NetApp云基础架构监控工具Cloud Insights支持您监控由Cloud Insights控制中心管理的Kubernetes集群的性能和利用率。Cloud Insights 将存储使用量与工作负载相关联。在 Astra 控制中心中启用 Cloud Insights 连接后，遥测信息将显示在 Astra 控制中心 UI 页面中。

Astra Control 接口

您可以使用不同的界面完成任务：

- * Web 用户界面（ UI ） *： Astra 控制服务和 Astra 控制中心使用同一个基于 Web 的 UI ，您可以在其中管理，迁移和保护应用程序。此外，还可以使用 UI 管理用户帐户和配置设置。
- * API *： Astra 控制服务和 Astra 控制中心使用相同的 Astra 控制 API 。使用 API ，您可以执行与使用 UI 相同的任务。

您还可以通过 Astra 控制中心管理，迁移和保护 VM 环境中运行的 Kubernetes 集群。

有关详细信息 ...

- "Astra Control Service 文档"
- "Astra 控制中心文档"
- "Astra Trident 文档"
- "使用 Astra Control API"
- "Cloud Insights 文档"
- "ONTAP 文档"

数据保护

了解 Astra 控制中心提供的数据保护类型，以及如何以最佳方式使用它们来保护您的应用程序。

快照，备份和保护策略

快照和备份均可保护以下类型的数据：

- 应用程序本身
- 与应用程序关联的任何永久性数据卷

- 属于应用程序的任何资源项目

snapshot 是应用程序的时间点副本，它与应用程序存储在同一个已配置卷上。通常速度较快。您可以使用本地快照将应用程序还原到较早的时间点。快照对于快速克隆很有用；快照包括应用程序的所有 Kubernetes 对象，包括配置文件。快照对于克隆或还原同一集群中的应用程序非常有用。

_backup_基于快照。它存储在外部对象存储中、因此、与本地快照相比、创建速度可能会较慢。您可以将应用程序备份还原到同一集群，也可以通过将应用程序备份还原到其他集群来迁移应用程序。您还可以选择较长的备份保留期限。由于备份存储在外部对象存储中，因此在发生服务器故障或数据丢失时，备份通常比快照提供更好的保护。

保护策略 _ 是一种通过根据您为应用程序定义的计划自动创建快照和 / 或备份来保护应用程序的方法。此外、您还可以通过保护策略选择要在计划中保留多少个快照和备份、并设置不同的计划粒度级别。使用保护策略自动执行备份和快照是确保每个应用程序根据组织的需求和服务级别协议(Service Level Agreement、SLA)要求进行保护的最佳方式。

> *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关联的永久性存储，则需要备份才能恢复。快照无法让您恢复。

克隆

_cloner_是应用程序、其配置及其永久性数据卷的精确副本。您可以在同一个 Kubernetes 集群或另一个集群上手动创建克隆。如果需要将应用程序和存储从一个 Kubernetes 集群移动到另一个 Kubernetes 集群，则克隆应用程序非常有用。

在存储后端之间进行复制

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。配置后、应用程序便可将数据和应用程序更改从一个存储后端复制到另一个存储后端、复制到同一集群上或复制到不同集群之间。

您可以在同一ONTAP集群或不同ONTAP集群上的两个ONTAP SVM之间进行复制。

Astra Control会将应用程序Snapshot副本异步复制到目标集群。复制过程包括SnapMirror复制的永久性卷中的数据以及受Astra Control保护的应用程序元数据。

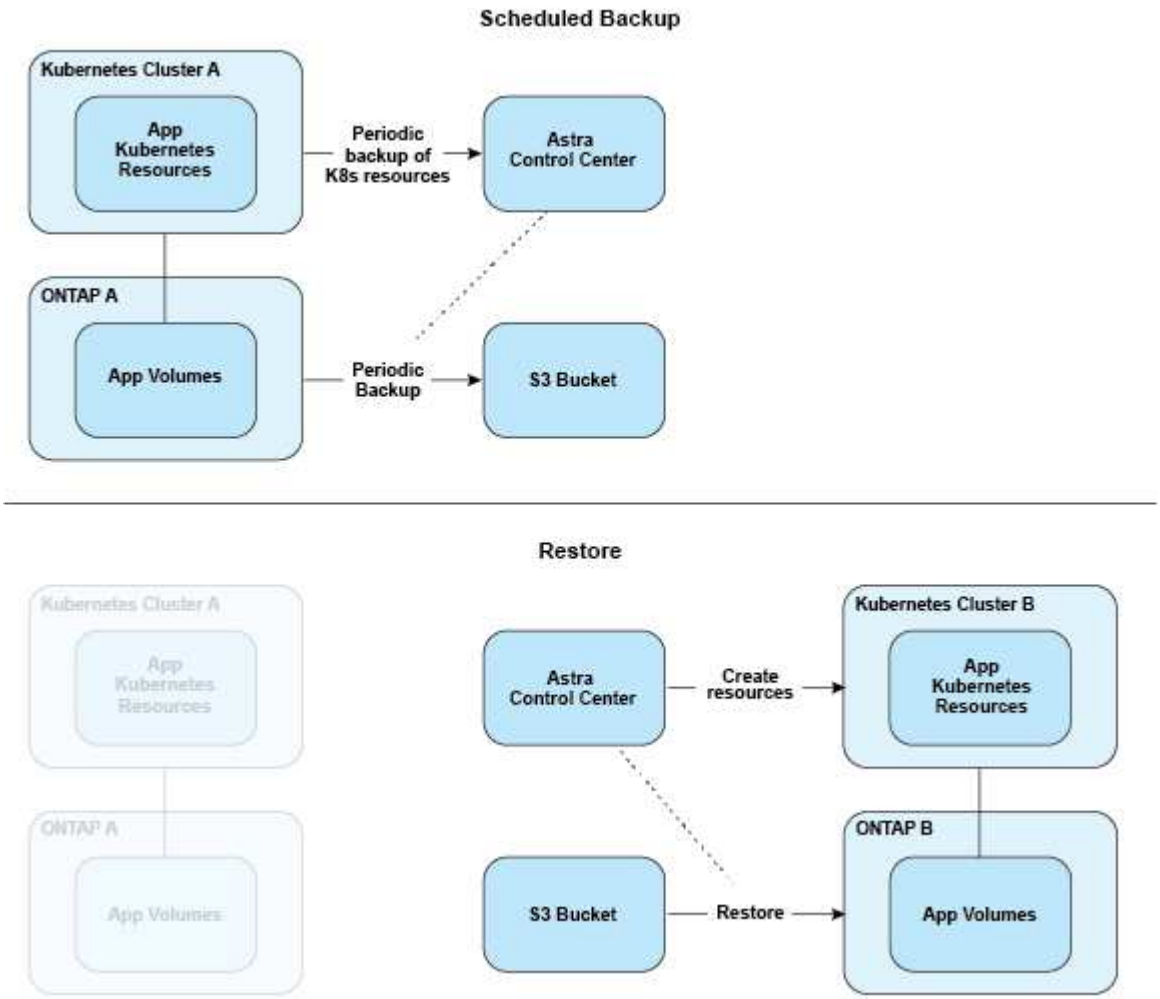
应用程序复制与应用程序备份和还原在以下方面有所不同：

- 应用程序复制：Astra Control要求源和目标Kubernetes集群(可以是同一集群)可用并进行管理、并将其各自的ONTAP存储后端配置为启用NetApp SnapMirror。Asta Control创建策略驱动型应用程序快照并将其复制到目标存储后端。NetApp SnapMirror技术用于复制永久性卷数据。要进行故障转移、Astra Control可以在目标Kubernetes集群上重新创建应用程序对象、并在目标ONTAP 集群上创建复制的卷、从而使复制的应用程序联机。由于目标ONTAP集群上已存在永久性卷数据、因此Astra Control可以为故障转移提供快速恢复时间。
- 应用程序备份和还原：备份应用程序时、Astra Control会创建应用程序数据的快照并将其存储在对象存储分段中。需要还原时、必须将存储分段中的数据复制到ONTAP 集群上的永久性卷。备份/还原操作不要求二级Kubernetes或ONTAP集群可用并进行管理、但额外的数据复制可能会导致还原时间较长。

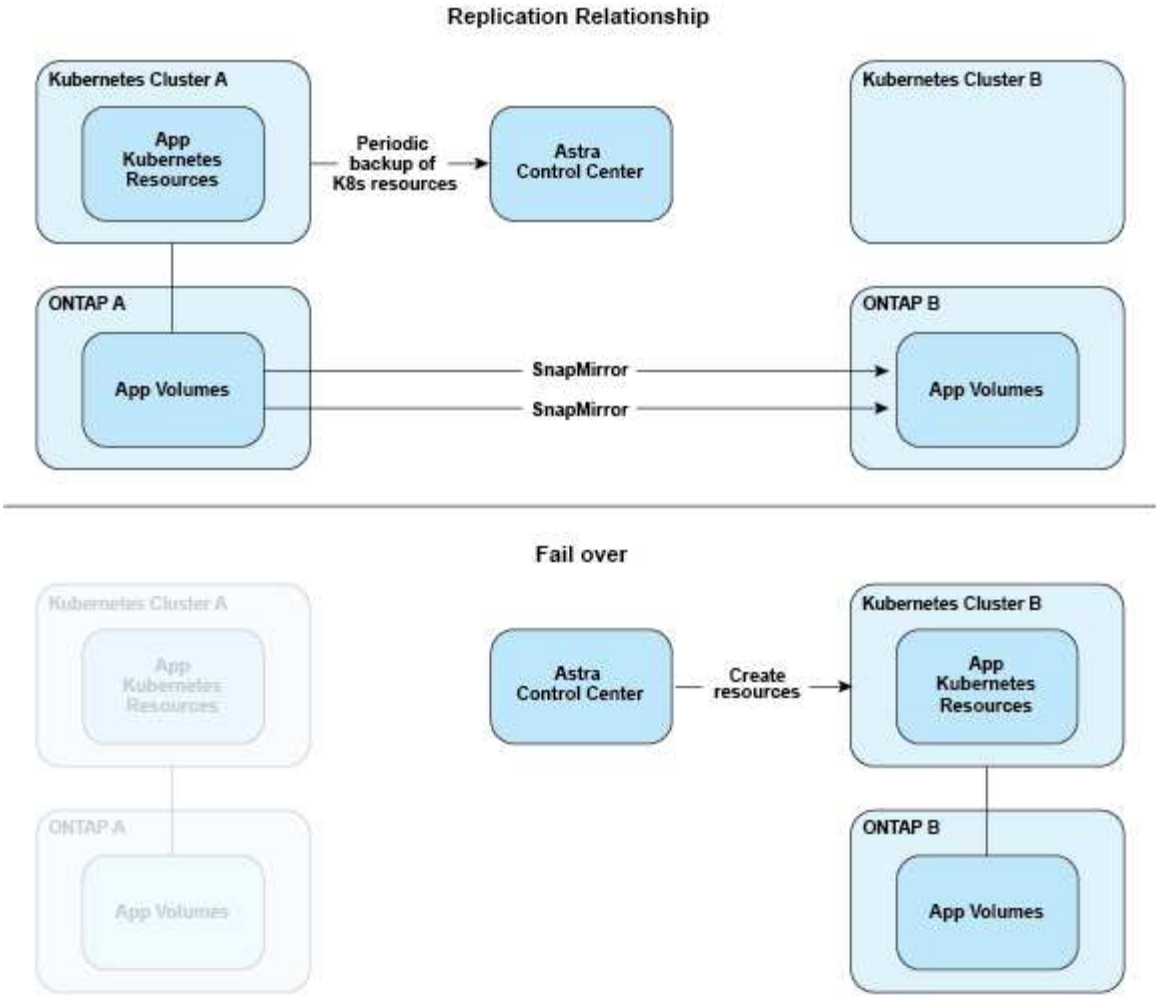
要了解如何复制应用程序、请参见 "使用SnapMirror技术将应用程序复制到远程系统"。

下图显示了计划的备份和还原过程与复制过程的对比情况。

备份过程会将数据复制到S3存储分段、并从S3存储分段进行还原：



另一方面、复制是通过复制到ONTAP来完成的、然后故障转移会创建Kubrenetes资源：



许可证已过期的备份、快照和克隆

如果许可证过期、只有当要添加或保护的应用程序是另一个Asta Control Center实例时、您才能添加新应用程序或执行应用程序保护操作(例如快照、备份、克隆和还原操作)。

许可

在部署Astra Control Center时、它会安装一个嵌入式90天评估版许可证、可用于4、800个CPU单元。如果您需要更多容量或更长的评估期、或者要升级到完整许可证、则可以从NetApp获得不同的评估许可证或完整许可证。

您可以通过以下方式之一获取许可证：

- 如果您正在评估Astra Control Center、并且需要与嵌入式评估许可证中包含的评估条款不同的评估条款、请与NetApp联系以申请不同的评估许可证文件。
- "如果您已购买Astra Control Center、请生成NetApp许可证文件(NLF)" 登录到NetApp 支持站点 并导航到"Systems"(系统)菜单下的软件许可证。

有关ONTAP 存储后端所需许可证的详细信息、请参见 "支持的存储后端"。

请确保您的许可证至少启用所需数量的CPU单元。如果Astra Control Center当前管理的CPU单元数超过所应用新许可证中的可用CPU单元数、您将无法应用新许可证。

评估版许可证和完全许可证

新安装的Astra Control Center会提供嵌入式评估许可证。评估版许可证可实现与完整许可证相同的功能和特性、有效期为90天。评估期结束后、需要完整许可证才能继续执行完整功能。

许可证到期

如果活动A作用 中的Astra Control Center许可证过期、则以下功能的UI和API功能将不可用：

- 手动创建本地快照和备份
- 计划本地快照和备份
- 从快照或备份还原
- 从快照或当前状态克隆
- 管理新应用程序
- 配置复制策略

如何计算许可证使用量

在将新集群添加到 Astra 控制中心时，只有在集群上运行的至少一个应用程序由 Astra 控制中心管理之后，该集群才会计入已用许可证。

开始管理集群上的应用程序时、该集群的所有CPU单元都会计入Astra Control Center许可证使用量中、但使用标签报告的Red Hat OpenShift集群节点CPU单元除外 `node-role.kubernetes.io/infra: ""`。

Red Hat OpenShift基础架构节点不使用Astra Control Center中的许可证。要将节点标记为基础架构节点、请应用此标签 `node-role.kubernetes.io/infra: ""` 连接到节点。

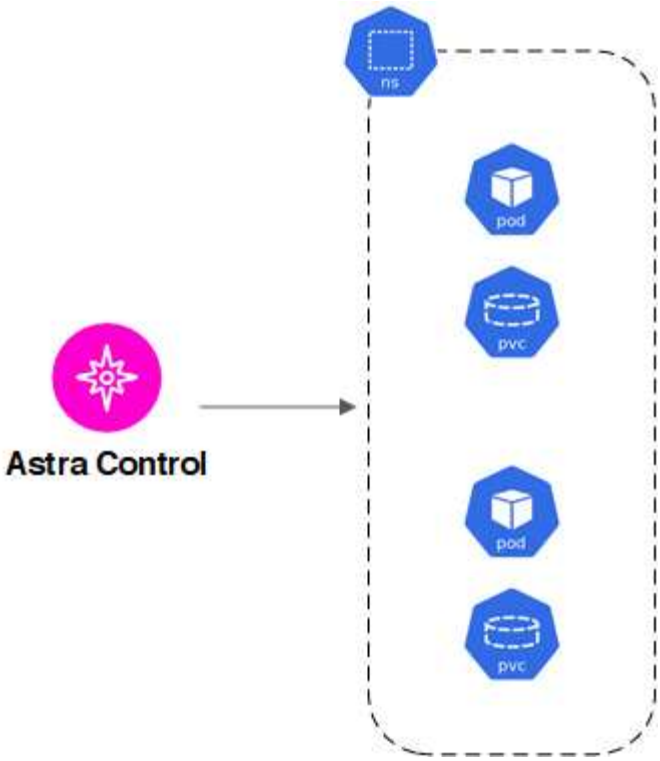
了解更多信息

- "首次设置Astra控制中心时添加许可证"
- "更新现有许可证"

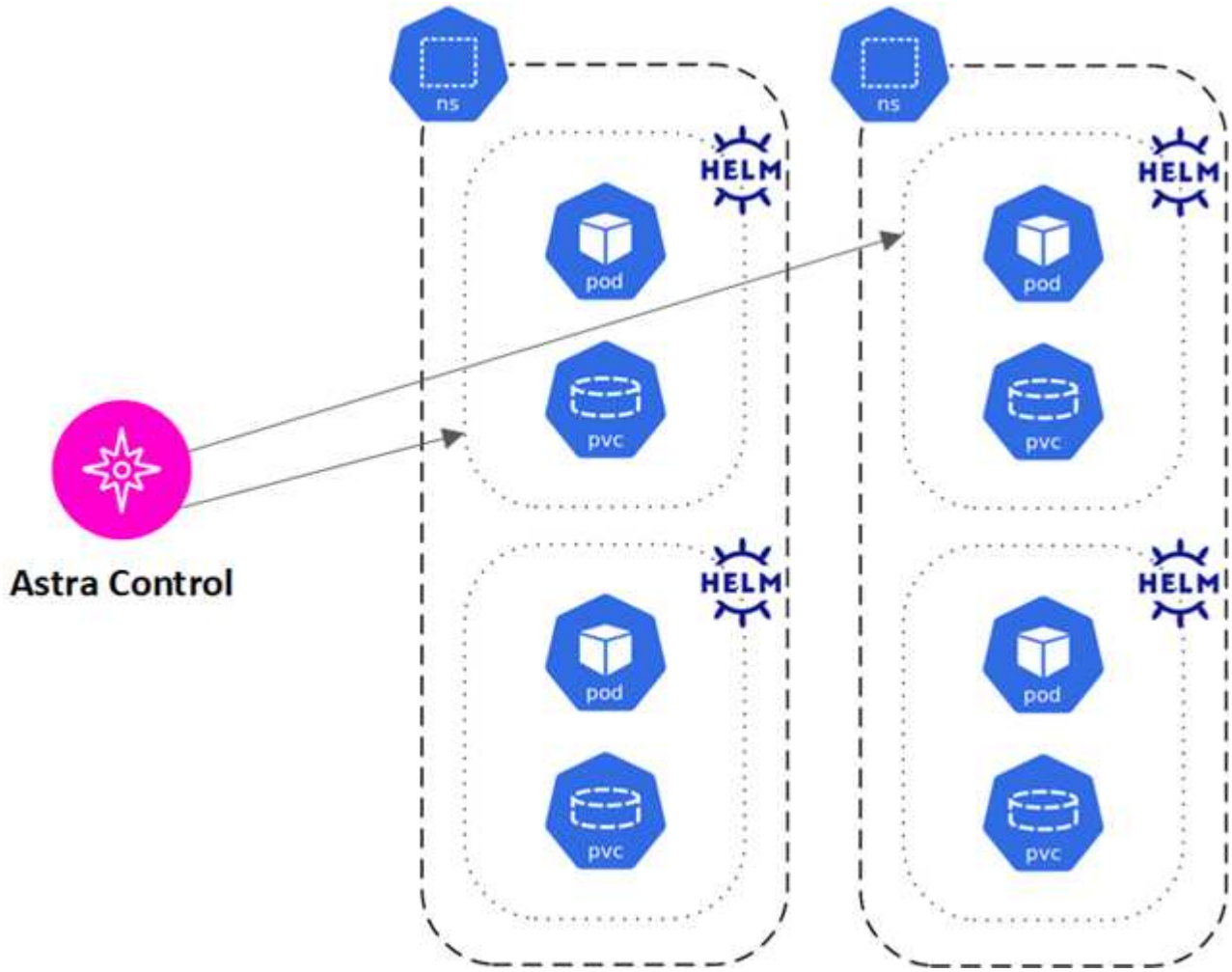
应用程序管理

当Astra Control发现集群时、这些集群上的应用程序将不受管理、直到您选择要如何管理它们为止。Astra Control 中的受管应用程序可以是以下任一项：

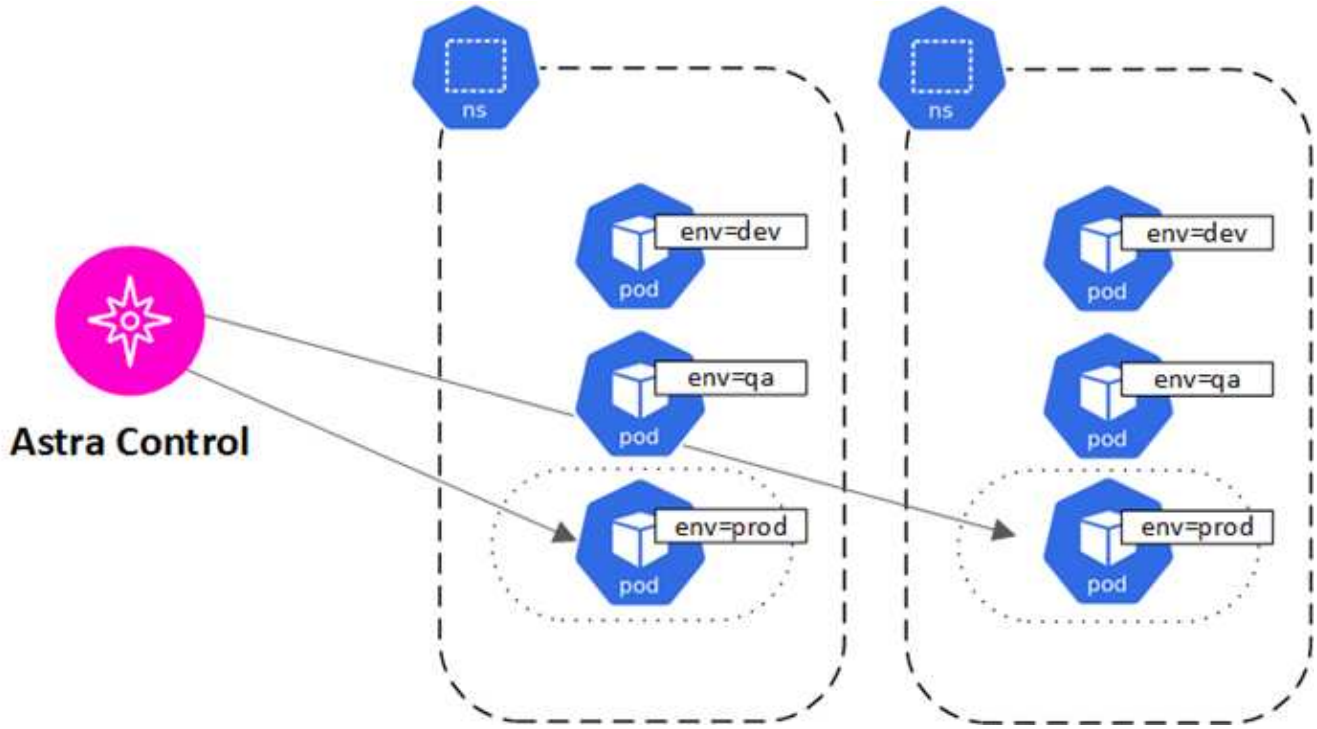
- 命名空间，包括该命名空间中的所有资源



- 部署在一个或多个命名空间中的单个应用程序(在此示例中使用了helm3)



- 一组通过一个或多个命名空间中的Kubernetes标签标识的资源



存储类和永久性卷大小

Astra控制中心支持NetApp ONTAP和Longhorn作为存储后端。

概述

Astra 控制中心支持以下功能：

- **Astra**三端存储类由**ONTAP** 存储提供支持：如果使用ONTAP 后端，Astra控制中心可以导入ONTAP 后端以报告各种监控信息。
- *Longhorn*支持的基于CSI的存储类：可以将Longhorn与Longhorn容器存储接口(CSI)驱动程序结合使用。

应在Asta Control Center之外预配置Asta三项存储类。

存储类

将集群添加到Astra控制中心时、系统会提示您选择该集群上先前配置的一个存储类作为默认存储类。如果在永久性卷请求（ PVC ）中未指定存储类，则会使用此存储类。可以随时在 Astra 控制中心内更改默认存储类，也可以随时通过在 PVC 或 Helm 图表中指定存储类的名称来使用任何存储类。确保您仅为 Kubernetes 集群定义了一个默认存储类。

有关详细信息 ...

- "Astra Trident 文档"

用户角色和命名空间

了解 Astra Control 中的用户角色和命名空间，以及如何使用它们控制对组织中资源的访问。

用户角色

您可以使用角色控制用户对 Astra Control 资源或功能的访问权限。以下是 Astra Control 中的用户角色：

- * 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。

您可以向 " 成员 " 或 " 查看器 " 用户添加限制，以将用户限制为一个或多个 [命名空间]。

命名空间

命名空间是指您可以分配给由 Astra Control 管理的集群中的特定资源的范围。将集群添加到 Astra Control 时，Astra Control 会发现集群的命名空间。发现后，可以将命名空间作为约束分配给用户。只有有权访问该命名空间的成员才能使用该资源。您可以使用命名空间来控制对资源的访问，方法是采用对您的组织有意义的模式；例如，按公司内的物理区域或部门进行访问。向用户添加约束时，您可以将该用户配置为可以访问所有命名空间或仅访问一组特定命名空间。您还可以使用命名空间标签分配命名空间约束。

了解更多信息

"管理本地用户和角色"

POD安全性

Astra控制中心通过POD安全策略(PSP)和POD安全允许(PSA)支持权限限制。通过这些框架、您可以限制哪些用户或组能够运行容器以及这些容器可以具有哪些权限。

某些Kubernetes分发版的默认POD安全配置可能限制性过大、并在安装Astra Control Center时导致问题。

您可以使用此处提供的信息和示例来了解Astra控制中心所做的POD安全更改、并使用POD安全方法来提供所需的保护、而不会干扰Astra控制中心的功能。

由Astra控制中心强制实施的PSAS

Asta Control Center可通过向安装Asta的命名空间(NetApp-ACC或自定义命名空间)以及为备份创建的命名空间添加以下标签来强制实施POD安全许可。

```
pod-security.kubernetes.io/enforce: privileged
```

由Astra控制中心安装的Psps

在Kubernetes 1.23或1.24上安装Astra Control Center时、会在安装期间创建多个POD安全策略。其中一些是永久性的、其中一些是在某些操作期间创建的、操作完成后会将其删除。当主机集群运行Kubernetes 1.25或更高版本时、Astra Control Center不会尝试安装PSP、因为这些版本不支持。

在安装期间创建的Psps

在安装Astra控制中心期间、Astra控制中心操作员会安装自定义POD安全策略A `Role` 对象和 `RoleBinding` 用于支持在Astra控制中心命名空间中部署Astra控制中心服务的对象。

新策略和对象具有以下属性：

```
kubectl get psp

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

kubectl get role -n <namespace_name>

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

kubectl get rolebinding -n <namespace_name>

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

备份操作期间创建的Psps

在备份操作期间、Astra控制中心会创建一个动态POD安全策略、即 `ClusterRole` 对象和 `RoleBinding` 对象。它们支持备份过程、该过程会在单独的命名空间中进行。

新策略和对象具有以下属性：

```
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 -n <namespace_name>

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

kubectl get rolebinding -n <namespace_name>

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

在集群管理期间创建的**Psps**

管理集群时、Astra控制中心会在受管集群中安装NetApp监控操作员。此运算符将创建一个POD安全策略、即 `ClusterRole` 对象和 `RoleBinding` 用于在Astra控制中心命名空间中部署遥测服务的对象。

新策略和对象具有以下属性：

```
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 -n <namespace_name>

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

kubectl get rolebinding -n <namespace_name>

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

版权信息

版权所有 © 2023 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。