概念
Astra Control Center

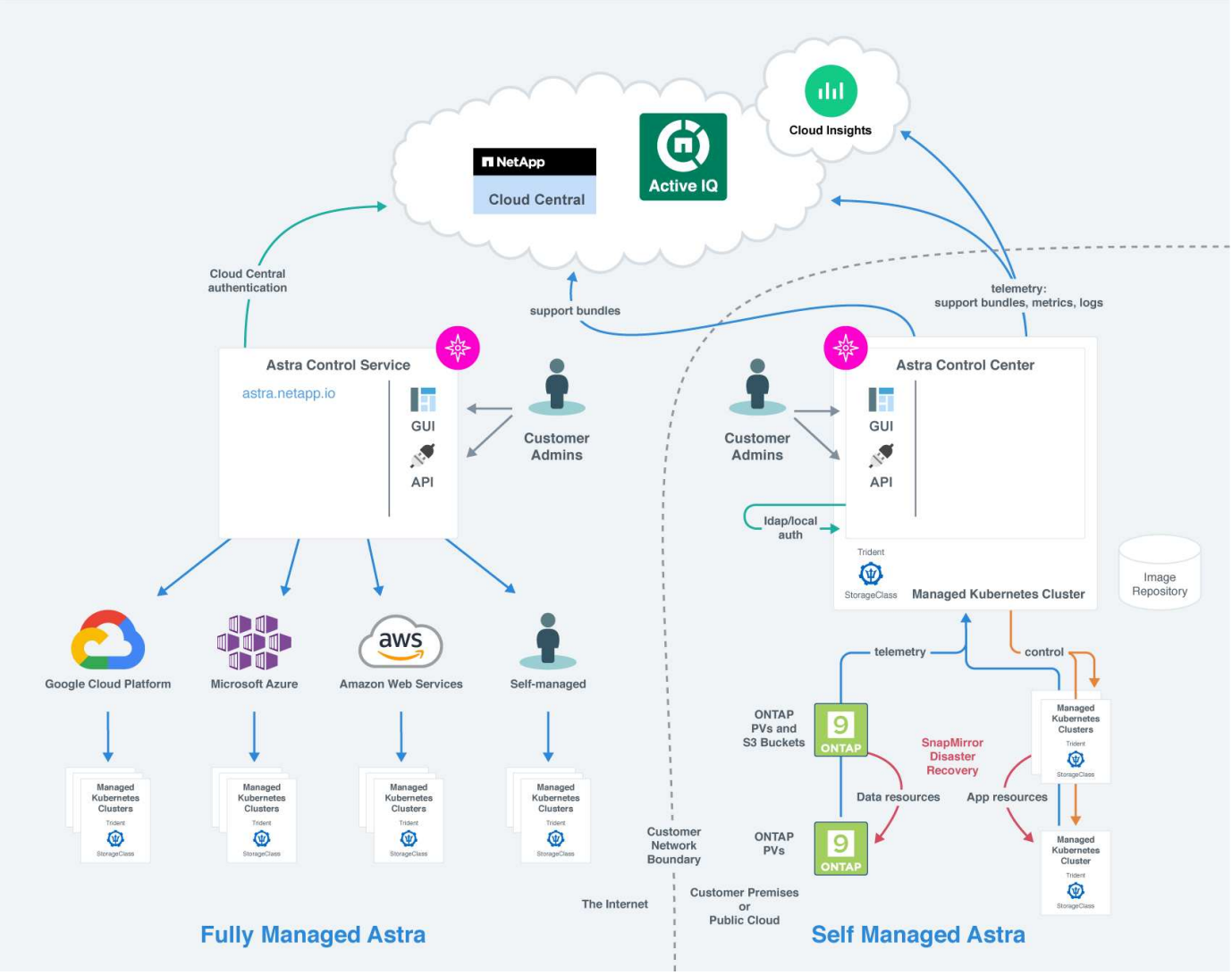
NetApp
November 27, 2023

目次

概念

アーキテクチャとコンポーネント

ここでは、 Astra Control 環境のさまざまなコンポーネントの概要を示します。



Astra Control コンポーネント

- * Kubernetes クラスタ * ： Kubernetes は、コンテナ化されたワークロードとサービスを管理するための、ポータブルで拡張性に優れたオープンソースプラットフォームであり、宣言型の設定と自動化の両方を促進します。Astra は、 Kubernetes クラスタでホストされているアプリケーションに管理サービスを提供します。
- * Trident * ：ネットアップが管理する、完全にサポートされているオープンソースのストレージプロビジョニングおよびオーケストレーションツールである Astra Trident を使用すると、 Docker と Kubernetes で管理されるコンテナ化アプリケーション用のストレージボリュームを作成できます。Astra Control Centerとともに導入した場合、Astra TridentにはONTAP ストレージバックエンドが設定されています。
- * ストレージバックエンド * ：

- Astra Control Serviceは、次のストレージバックエンドを使用します。
  - "NetApp Cloud Volumes Service for Google Cloud" または、GKEクラスタのストレージバックエンドとしてGoogle Persistent Diskを使用します
  - "Azure NetApp Files の特長" またはAzure Managed DisksをAKSクラスタのストレージバックエンドとして使用します。
  - "Amazon Elastic Block Store（EBS）" または "NetApp ONTAP 対応の Amazon FSX" EKSクラスタのバックエンドストレージオプションとして使用できます。
- Astra Control Center は、次のストレージバックエンドを使用します。
  - ONTAP AFF 、FAS 、およびASA 。ONTAP は、ストレージソフトウェアおよびハードウェアプラットフォームとして、コアストレージサービス、複数のストレージアクセスプロトコルのサポート、 Snapshot やミラーリングなどのストレージ管理機能を提供します。
  - Cloud Volumes ONTAP

- * Cloud Insights *：NetAppクラウドインフラ監視ツールであるCloud Insightsを使用すると、Astra Control Centerで管理されるKubernetesクラスタのパフォーマンスと利用率を監視できます。Cloud Insights ：ストレージ使用率とワークロードの相関関係を示します。Cloud Insights 接続を Astra コントロールセンターで有効にすると、テレメータの情報が Astra コントロールセンターの UI ページに表示されます。

Astra Control インターフェイス

さまざまなインターフェイスを使用してタスクを完了できます。

- * ウェブユーザーインタフェース（ UI ） * ： Astra Control Service と Astra Control Center の両方が、同じ Web ベースの UI を使用して、アプリケーションの管理、移行、保護を行うことができます。また、 UI を使用してユーザアカウントと設定を管理することもできます。
- * API* ： Astra Control Service と Astra Control Center は、どちらも同じ Astra Control API を使用します。API を使用するタスクは、 UI を使用するタスクと同じです。

Astra Control Center を使用すると、 VM 環境内で実行される Kubernetes クラスタを管理、移行、保護することもできます。

を参照してください。

- "Astra Control Service のマニュアル"
- "Astra Control Center のドキュメント"
- "Astra Trident のドキュメント"
- "Astra Control API を使用"
- "Cloud Insights のドキュメント"
- "ONTAP のドキュメント"

データ保護

Astra Control Center で使用可能なデータ保護の種類と、それらを使用してアプリケーションを保護する最適な方法について説明します。

Snapshot 、バックアップ、保護のポリシー

Snapshotとバックアップのどちらも、次のタイプのデータを保護します。

- アプリケーション自体
- アプリケーションに関連付けられている永続的データボリューム
- アプリケーションに属するリソースアーティファクト

a_snapshot_は 、アプリケーションと同じプロビジョニングボリュームに格納されるアプリケーションのポイントインタイムコピーです。通常は高速です。ローカル Snapshot を使用して、アプリケーションを以前の時点にリストアできます。スナップショットは高速クローンに便利です。スナップショットには、構成ファイルを含む、アプリケーションのすべての Kubernetes オブジェクトが含まれます。スナップショットは、同じクラスタ内でアプリケーションをクローニングまたはリストアする場合に便利です。

_backup_はSnapshotに基づいています。外部のオブジェクトストアに格納されるため、ローカルSnapshotに比べて取得に時間がかかることがあります。アプリケーションのバックアップを同じクラスタにリストアすることも、バックアップを別のクラスタにリストアして移行することもできます。バックアップの保持期間を延長することもできます。バックアップは外部のオブジェクトストアに格納されるため、サーバで障害が発生したりデータが失われたりした場合に備えて、 Snapshot よりも優れた保護機能を提供できます。

a_protection policy__ は、アプリケーション用に定義したスケジュールに従って、スナップショット、バックアップ、またはその両方を自動的に作成することで、アプリケーションを保護する方法です。また、保護ポリシーでは、スケジュールで保持するSnapshotとバックアップの数を選択したり、さまざまなスケジュールレベルを設定したりすることもできます。保護ポリシーを使用してバックアップとスナップショットを自動化することは、組織のニーズやSLA（Service Level Agreement）の要件に応じて各アプリケーションを確実に保護するための最良の方法です。

> _ 最新のバックアップがあるまで、完全に保護することはできません _ 。これは、永続ボリュームから離れたオブジェクトストアにバックアップが格納されるために重要です。障害または事故によってクラスタとその永続的ストレージが消去された場合は、バックアップをリカバリする必要があります。Snapshot を使用してリカバリすることはできません。

クローン

a_clone_は、アプリケーション、その設定、および永続データボリュームの完全な複製です。クローンは、同じ Kubernetes クラスタまたは別のクラスタに手動で作成できます。アプリケーションとストレージを Kubernetes クラスタ間で移動する必要がある場合は、アプリケーションをクローニングすると便利です。

ストレージバックエンド間のレプリケーション

Astra Controlを使用すると、NetApp SnapMirrorテクノロジの非同期レプリケーション機能を使用して、RPO（目標復旧時点）とRTO（目標復旧時間）の低いアプリケーションのビジネス継続性を構築できます。設定が完了すると、アプリケーションは、ストレージバックエンド間、同じクラスタ上、または異なるクラスタ間でデータやアプリケーションの変更をレプリケートできるようになります。

レプリケートは、同じONTAPクラスタ上または異なるONTAPクラスタ上の2つのONTAP SVM間で実行できます。

Astra Controlは、アプリケーションのSnapshotコピーをデスティネーションクラスタに非同期でレプリケートします。レプリケーションプロセスには、SnapMirrorでレプリケートされた永続ボリュームのデータと、Astra Controlで保護されたアプリケーションメタデータが含まれます。

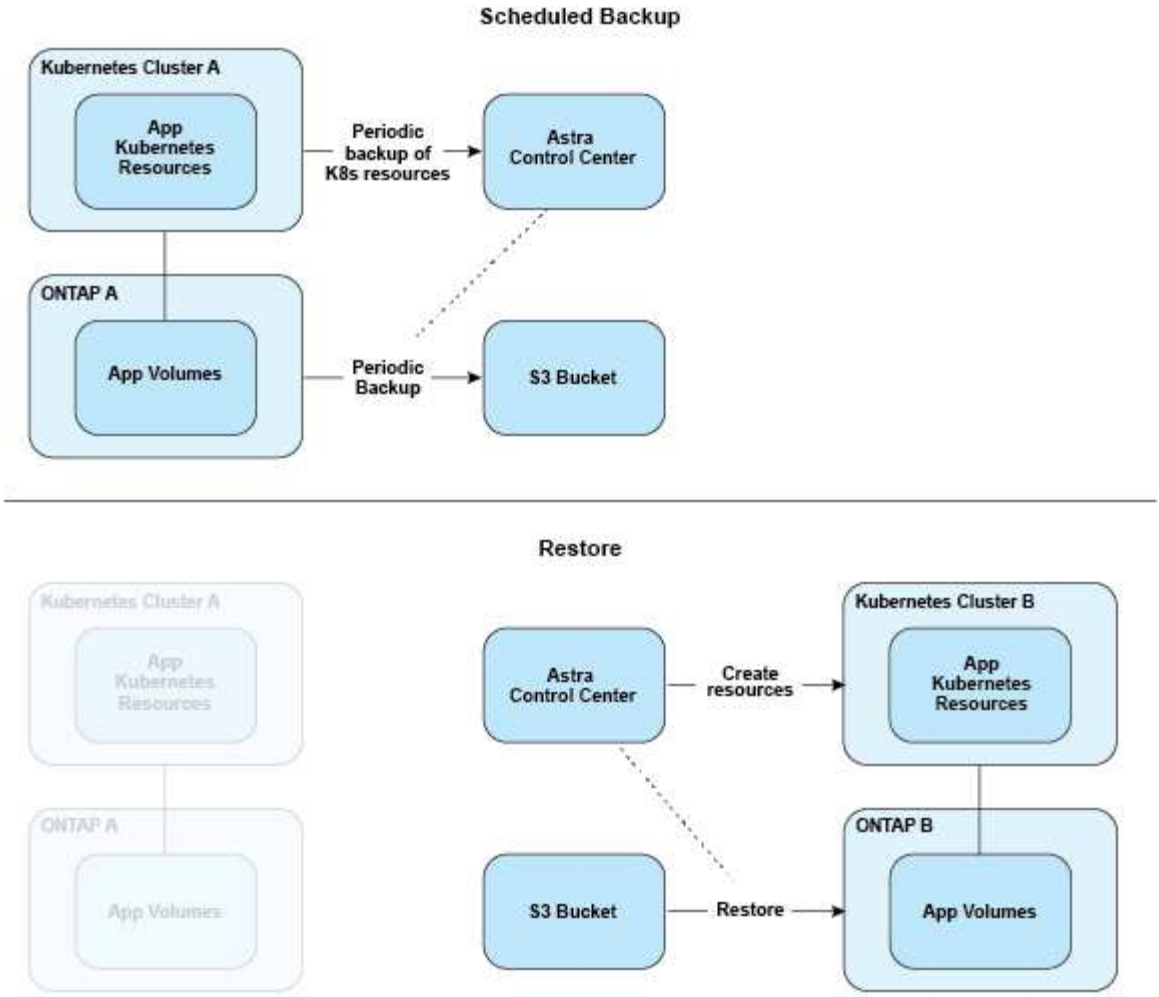
アプリケーションのレプリケーションは、次のようにアプリケーションのバックアップとリストアとは異なります。

- アプリケーションレプリケーション：Astra Controlを使用するには、ソースとデスティネーションのKubernetesクラスタ（同じクラスタでも可）が使用可能で、それぞれのONTAPストレージバックエンドでNetApp SnapMirrorを有効にするように設定されている必要があります。Astra Controlは、ポリシーベースのアプリケーションSnapshotを作成し、デスティネーションストレージバックエンドにレプリケートします。NetApp SnapMirrorテクノロジは、永続ボリュームのデータのレプリケートに使用されます。フェイルオーバーのために、デスティネーションONTAP クラスタ上のレプリケートされたボリュームを含むデスティネーションKubernetesクラスタにアプリケーションオブジェクトを再作成することで、レプリケーションされたアプリケーションをオンラインにすることができます。永続ボリュームのデータはデスティネーションのONTAPクラスタにすでに存在するため、Astra Controlを使用してフェイルオーバー時に短時間でリカバリできます。
- アプリケーションのバックアップとリストア：アプリケーションのバックアップ時に、Astra Controlによってアプリケーションデータのスナップショットが作成され、オブジェクトストレージバケットに格納されます。リストアが必要な場合は、バケット内のデータをONTAP クラスタ上の永続ボリュームにコピーする必要があります。バックアップ/リストア処理では、セカンダリKubernetes / ONTAPクラスタを使用可能にして管理する必要はありませんが、データコピーを追加するとリストア時間が長くなる可能性があります。

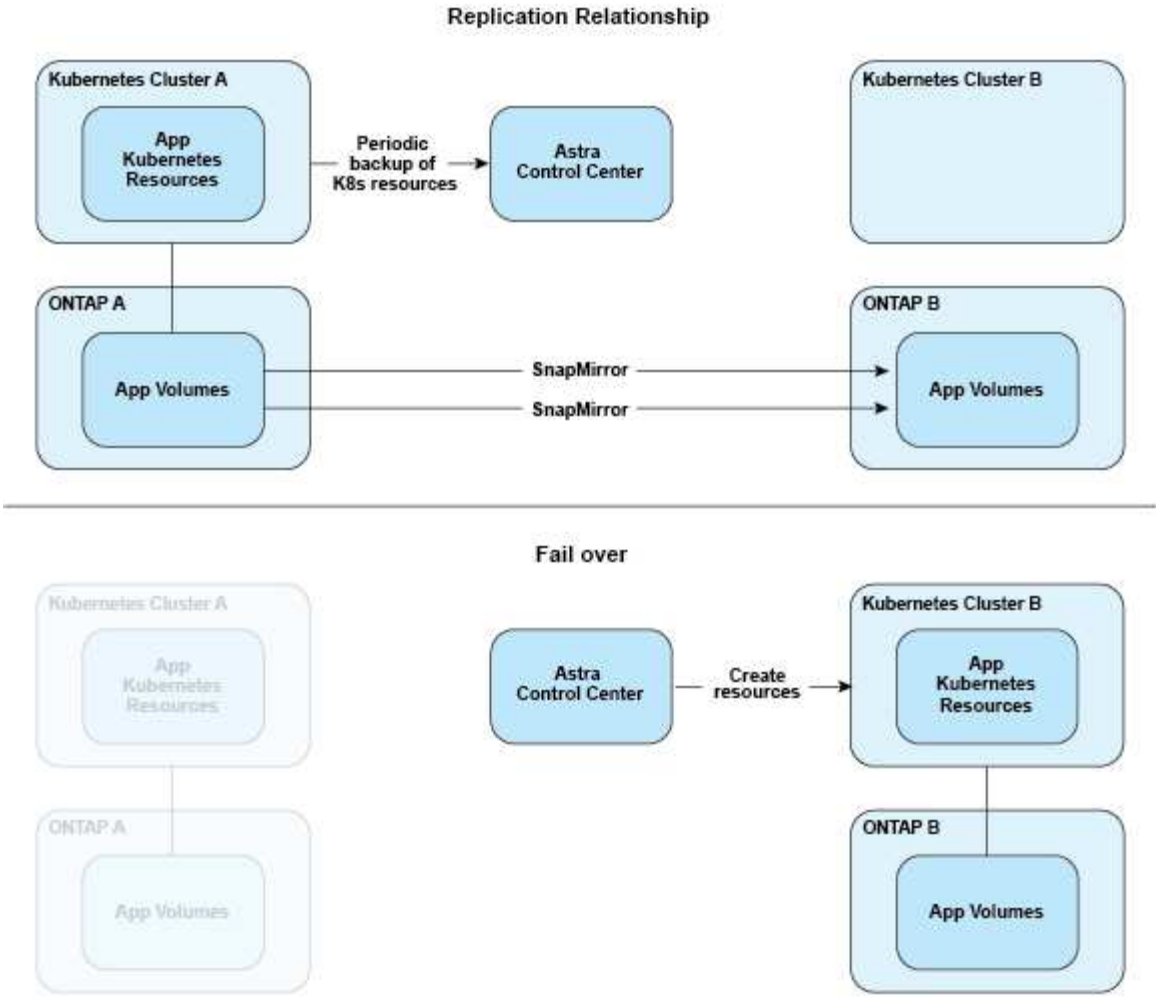
アプリケーションを複製する方法については、を参照してください "SnapMirrorテクノロジを使用してアプリケーションをリモートシステムにレプリケート"。

次の図は、スケジュールされたバックアップおよびリストアのプロセスをレプリケーションプロセスと比較したものです。

バックアッププロセスでは、S3バケットにデータをコピーし、S3バケットからリストアします。



一方、レプリケーションはONTAPにレプリケートすることで実行され、フェイルオーバーによってKubernetesリソースが作成されます。



ライセンスの有効期限が切れたバックアップ、スナップショット、クローン

ライセンスの有効期限が切れた場合、追加または保護するアプリケーションが別のAstra Control Centerインスタンスである場合にのみ、新しいアプリケーションの追加やアプリケーションの保護処理（Snapshot、バックアップ、クローン、リストア処理など）を実行できます。

ライセンス

Astra Control Centerを導入すると、4、800 CPUユニットの90日間の評価ライセンスが組み込まれてインストールされます。容量の追加や評価期間の延長が必要な場合、またはフルライセンスにアップグレードする場合は、ネットアップから別の評価用ライセンスまたはフルライセンスを取得できます。

次のいずれかの方法でライセンスを取得します。

- Astra Control Centerを評価する際に、組み込みの評価用ライセンスと異なる評価条件が必要な場合は、ネットアップに連絡して別の評価用ライセンスファイルをリクエストしてください。
- "Astra Control Centerを購入済みの場合は、ネットアップライセンスファイル（NLF）を生成する" NetApp Support Site にログインし、[Systems]メニューからソフトウェアライセンスに移動します。

ONTAP ストレージバックエンドに必要なライセンスの詳細については、を参照してください "サポートされるストレージバックエンド"。

> ライセンスで有効になっているCPUユニットが必要な数以上であることを確認してください。Astra Control Centerで現在管理しているCPUユニット数が、適用する新しいライセンスで使用可能なCPUユニット数を超えると、新しいライセンスを適用できなくなります。

評価用ライセンスとフルライセンス

Astra Control Centerの新しいインストールには、評価用ライセンスが組み込まれています。評価用ライセンスでは、フルライセンスと同じ機能を制限付き（90日間）で使用できます。評価期間が終了したら、フル機能を使用するにはフルライセンスが必要です。

ライセンスの有効期限

アクティブなAstra Control Centerのライセンスが期限切れになると、次の機能のUIおよびAPI機能は使用できなくなります。

- ローカルのスナップショットとバックアップを手動で実行します
- スケジュールされたローカルSnapshotおよびバックアップ
- Snapshot またはバックアップからのリストア
- Snapshot または現在の状態からクローニングしています
- 新しいアプリケーションの管理
- レプリケーションポリシーを設定しています

ライセンス消費量の計算方法

新しいクラスタを Astra Control Center に追加しても、クラスター上で実行されているアプリケーションの少なくとも 1 つが Astra Control Center によって管理されるまで、使用済みのライセンスにはカウントされません。

クラスタでアプリケーションの管理を開始すると、そのクラスタのすべてのCPUユニットがAstra Control Centerのライセンス消費に含まれます。ただし、でラベルを使用して報告されるRed Hat OpenShiftクラスタノードのCPUユニットは除きます `node-role.kubernetes.io/infra: ""`。

> Red Hat OpenShiftインフラノードでは、Astra Control Centerのライセンスは使用されません。ノードをインフラストラクチャノードとしてマークするには、ラベルを適用します `node-role.kubernetes.io/infra: ""` ノードに追加します。

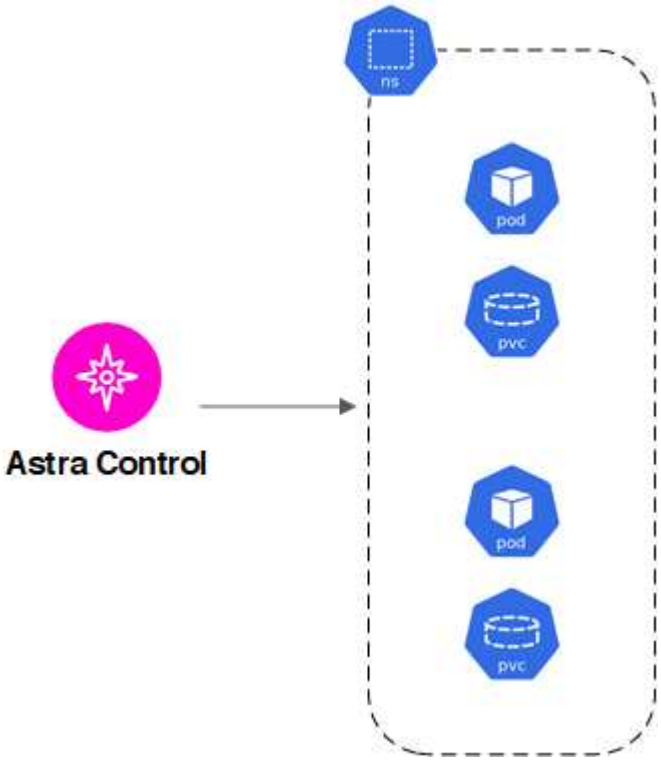
詳細については、こちらをご覧ください

- "Astra Control Centerの初回セットアップ時にライセンスを追加します"
- "既存のライセンスを更新する"

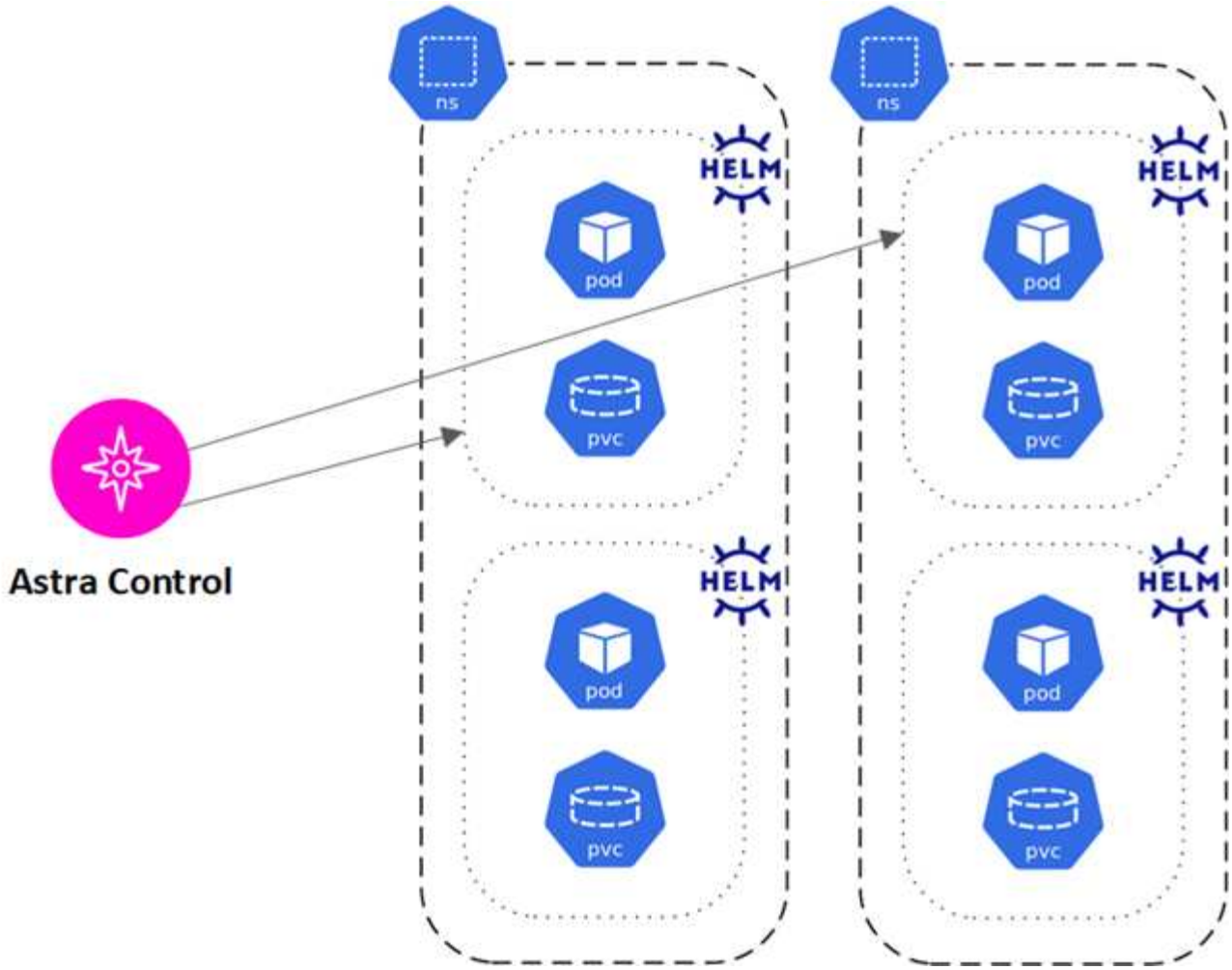
アプリケーション管理

Astra Controlがクラスタを検出すると、それらのクラスタ上のアプリケーションは、管理方法を選択するまで管理されません。Astra Control のマネージドアプリケーションには、次のいずれかを使用できます。

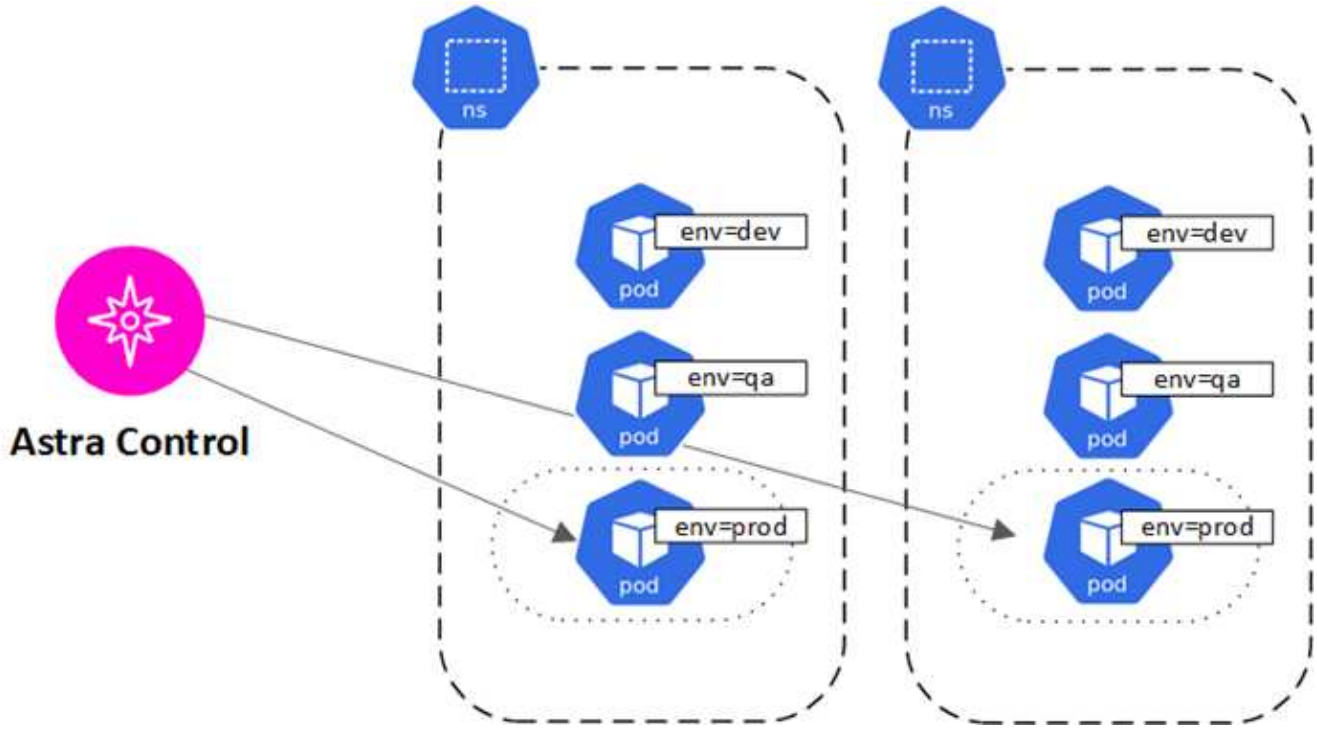
- ネームスペース。ネームスペース内のすべてのリソースを含みます



- 1つ以上のネームスペース内に導入された個 々 のアプリケーション（この例では、helm3を使用）



- 1つ以上のネームスペース内のKubernetesラベルで識別されるリソースのグループ



ストレージクラスと永続的ボリュームサイズ

Astra Control Centerでは、NetApp ONTAPとLonghornがストレージバックエンドとしてサポートされます。

概要

Astra Control Center は、次の機能をサポートします。

- * ONTAP ストレージを基盤とするAstra Tridentストレージクラス*：ONTAP バックエンドを使用している場合、Astra Control CenterでONTAP バックエンドをインポートしてさまざまな監視情報をレポートすることができます。
- **Longhorn**によってサポートされる**CSI**ベースのストレージクラス: Longhorn Container Storage Interface (CSI)ドライバでLonghornを使用できます。

> Astra Tridentのストレージクラスは、Astra Control Center以外で事前に設定する必要があります。

ストレージクラス

Astra Control Centerにクラスタを追加する場合は、そのクラスタで以前に設定したストレージクラスをデフォルトのストレージクラスとして選択するように求められます。このストレージクラスは、永続ボリューム要求（ PVC ）でストレージクラスが指定されていない場合に使用されます。デフォルトのストレージクラスは、 Astra Control Center 内でいつでも変更できます。また、 PVC または Helm チャート内のストレージクラスの名前を指定することで、任意のストレージクラスをいつでも使用できます。Kubernetes クラスタにデフォルトのストレージクラスが 1 つだけ定義されていることを確認します。

を参照してください。

- "Astra Trident のドキュメント"

ユーザロールとネームスペース

Astra Control のユーザロールとネームスペースについて説明し、それらを使用して組織内のリソースへのアクセスを制御する方法を説明します。

ユーザロール

ロールを使用して、ユーザが Astra Control のリソースまたは機能にアクセスできるように制御できます。Astra Control のユーザロールは次のとおりです。

- * Viewer * はリソースを表示できます。
- メンバー * には、ビューア・ロールの権限があり、アプリとクラスタの管理、アプリの管理解除、スナップショットとバックアップの削除ができます。
- **Admin** にはメンバーの役割権限があり、 Owner 以外の他のユーザーを追加および削除できます。
- * Owner * には Admin ロールの権限があり、任意のユーザーアカウントを追加および削除できます。

メンバーまたはビューアユーザーに制約を追加して、ユーザーを 1 つ以上に制限できます [ネームスペース]。

ネームスペース

ネームスペースは、 Astra Control によって管理されるクラスタ内の特定のリソースに割り当てることができるスコープです。Astra Control では、 Astra Control にクラスタを追加すると、クラスタのネームスペースが検出されます。検出されたネームスペースは、ユーザに制約として割り当てることができます。そのリソースを使用できるのは、そのネームスペースにアクセスできるメンバーだけです。名前空間を使用すると、組織に適したパラダイム（たとえば、会社内の物理的なリージョンや部門）を使用して、リソースへのアクセスを制御できます。ユーザに制約を追加する場合は、そのユーザにすべてのネームスペースへのアクセス権を設定するか、特定のネームスペースのセットのみを設定できます。ネームスペースラベルを使用して、ネームスペースの制約を割り当てることもできます。

詳細については、こちらをご覧ください

"ローカルユーザとロールを管理します"

ポッドセキュリティ

Astra Control Centerは、PoDセキュリティポリシー（PSP）およびPoDセキュリティアドミッション（PSA）による特権制限をサポートします。これらのフレームワークを使用すると、ユーザまたはグループがコンテナを実行できる対象や、コンテナに付与できる権限を制限できます。

Kubernetesディストリビューションの中には、デフォルトのポッドセキュリティ構成が用意されているものがあり、制限が厳しく、Astra Control Centerのインストール時に問題が発生する場合があります。

ここに記載されている情報と例を使用して、Astra Control Centerが行うポッドのセキュリティの変更を理解し、Astra Control Centerの機能を妨げずに必要な保護を提供するポッドのセキュリティアプローチを使用できます。

Astra Control Centerによって強制されるPSAS

Astra Control Centerでは、Astraがインストールされているネームスペース（netapp-accまたはカスタムネームスペース）とバックアップ用に作成されたネームスペースに次のラベルを追加することで、ポッドのセキュリティアドミッションを適用できます。

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

Astra Control Centerによってインストールされた**PSP**

Kubernetes 1.23または1.24にAstra Control Centerをインストールすると、インストール時にいくつかのポッドセキュリティポリシーが作成されます。これらの中には永続的なものもあれば、一部のものは特定の処理中に作成され、処理が完了すると削除されます。ホストクラスタでKubernetes 1.25以降が実行されている場合、これらのバージョンではサポートされていないため、Astra Control CenterはPSPのインストールを試みません。

インストール中に作成された**PSP**

Astra Control Centerのインストール中、Astra Control CenterオペレータはカスタムポッドセキュリティポリシーAをインストールします `Role` オブジェクト、および `RoleBinding` Astra Control Centerネームスペースへの Astra Control Centerサービスの導入をサポートするオブジェクト。

新しいポリシーとオブジェクトには次の属性があります。

```
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
```

バックアップ処理中に作成された**PSP**

バックアップ操作中に、Astra Control Centerは動的なポッドセキュリティポリシーAを作成します `ClusterRole` オブジェクト、および `RoleBinding` オブジェクト。これらの機能により、別のネームスペースで実行されるバックアッププロセスがサポートされます。

新しいポリシーとオブジェクトには次の属性があります。

```
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
```

クラスタ管理中に作成された**PSP**

クラスターを管理する場合、Astra Control Centerは管理対象クラスタにNetApp Monitoringオペレータをインストールします。この演算子は、ポッドセキュリティポリシーAを作成します `ClusterRole` オブジェクト、および `RoleBinding` テレメトリサービスをAstra Control Center名前空間に展開するオブジェクト。

新しいポリシーとオブジェクトには次の属性があります。

```
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
```