Documentación de Astra Control Service

Astra Control Service

NetApp
April 24, 2024

Tabla de contenidos

Documentación de Astra Control Service

Notas de la versión

Novedades de Astra Control Service

NetApp actualiza periódicamente Astra Control Service para ofrecerle nuevas funciones, mejoras y correcciones de errores.

14 de marzo de 2024

(Vista previa técnica) Flujos de trabajo declarativos de Kubernetes

Esta versión de Astra Control Center contiene la funcionalidad declarativa de Kubernetes que le permite realizar una gestión de datos desde un recurso personalizado de Kubernetes nativo (CR).

Esta funcionalidad solo está disponible en la instancia del programa de primera adopción (EAP) de Astra Control Service. Póngase en contacto con su representante de ventas de NetApp para obtener información sobre cómo unirse al EAP.

Después de instalar el "Conector Astra" En el clúster que desee gestionar, podrá realizar las siguientes operaciones de clúster basadas en CR en la interfaz de usuario o desde un CR:

- "Defina una aplicación mediante un recurso personalizado"
- "Defina el período"
- "Proteja todo un clúster"
- "Realice una copia de seguridad de su aplicación"
- "Crear una copia de Snapshot"
- "Crear programaciones para Snapshot o backups"
- "Restaure una aplicación desde una copia Snapshot o un backup"

7 de noviembre de 2023

Nuevas funciones y soporte

- * Capacidades de copia de seguridad y restauración para aplicaciones con backends de almacenamiento respaldados por controladores de economía ontap-nas*: Permite operaciones de copia de seguridad y restauración para `ontap-nas-economy` con algunos "sencillos pasos".
- **Soporte de Astra Control Service para clústeres locales de Red Hat OpenShift Container Platform**

  "Añadir un clúster"

- **Copias de seguridad inmutables**: Astra Control ahora es compatible "backups de solo lectura que se pueden modificar" como capa de seguridad adicional contra el malware y otras amenazas.
- **Presentamos Astra Control Provisionador**

  Con el lanzamiento 23,10, Astra Control introduce un nuevo componente de software llamado Astra Control Provisioning que estará disponible para todos los usuarios con licencia de Astra Control. Astra Control Provisioning ofrece acceso a un superconjunto de funciones avanzadas de aprovisionamiento de almacenamiento y gestión más allá de las que ofrece Astra Trident. Estas funciones están disponibles para todos los clientes de Astra Control sin coste adicional.

- **Empieza con Astra Control Provisioner**
  Puede hacerlo "Habilita el aprovisionador de Astra Control" Si ha instalado y configurado su entorno de modo que utilice Astra Trident 23,10.
- **La funcionalidad de Astra Control Provisionador**

  Las siguientes funciones están disponibles en la versión Astra Control Provisioner 23,10:

  - * Seguridad de backend de almacenamiento mejorada con cifrado Kerberos 5*: Puede mejorar la seguridad del almacenamiento "habilitar cifrado" para el tráfico entre el clúster gestionado y el back-end de almacenamiento. El aprovisionador de control de Astra admite el cifrado de Kerberos 5 a través de conexiones NFSv4,1 GbE desde clústeres de Red Hat OpenShift a volúmenes Azure NetApp Files y ONTAP en las instalaciones.
  - **Recuperar datos usando una instantánea**: Astra Control Provisioner proporciona una restauración de volumen rápida y en el lugar desde una instantánea usando el `TridentActionSnapshotRestore` (TASR) CR.
  - * Capacidades de copia de seguridad y restauración para aplicaciones con `ontap-nas-economy` Back-ends de almacenamiento respaldados por el conductor*: Como se describe anterior.

- **Soporte de Astra Control Service para Red Hat OpenShift Service en clústeres de AWS (ROSA)**

  "Añadir un clúster"

- **Soporte para la gestión de aplicaciones que utilizan almacenamiento NVMe/TCP**
  Astra Control ahora puede gestionar aplicaciones respaldadas por volúmenes persistentes que están conectados mediante NVMe/TCP.
- * Ganchos de ejecución desactivados por defecto*: A partir de esta versión, la funcionalidad de los ganchos de ejecución puede ser "activado" o desactivado para seguridad adicional (está desactivado de forma predeterminada). Si todavía no has creado enlaces de ejecución para usarlos con Astra Control, debes hacerlo "active la función de enlaces de ejecución" para empezar a crear ganchos. Si ha creado enlaces de ejecución antes de esta versión, la funcionalidad de enlaces de ejecución permanece activada y puede utilizar los enlaces como lo haría normalmente.

2 de octubre de 2023

Nuevas funciones y soporte

Esta es una versión de corrección de errores menor.

27 de julio de 2023

Nuevas funciones y soporte

- Ahora las operaciones de clonado admiten solo clones activos (estado actual de la aplicación gestionada). Para clonar desde una copia de Snapshot o un backup, use el flujo de trabajo de restauración.

  "Restaurar aplicaciones"

26 de junio de 2023

Nuevas funciones y soporte

- Las suscripciones de Azure Marketplace ahora se facturan por hora en lugar de por minuto

  "Configurar facturación"

30 de mayo de 2023

Nuevas funciones y soporte

- Compatibilidad con clústeres privados de Amazon EKS

  "Gestione clústeres privados desde Astra Control Service"

- Compatibilidad para seleccionar la clase de almacenamiento de destino durante las operaciones de restauración o clonado

  "Restaurar aplicaciones"

15 de mayo de 2023

Nuevas funciones y soporte

Esta es una versión de corrección de errores menor.

25 de abril de 2023

Nuevas funciones y soporte

- Compatibilidad con clústeres privados de Red Hat OpenShift

  "Gestione clústeres privados desde Astra Control Service"

- Soporte para incluir o excluir recursos de aplicaciones durante las operaciones de restauración

  "Restaurar aplicaciones"

- Compatibilidad para la gestión de aplicaciones solo de datos

  "Inicie la gestión de aplicaciones"

17 de enero de 2023

Nuevas funciones y soporte

- Funciones mejoradas de enlaces de ejecución con opciones de filtrado adicionales

  "Gestione los enlaces de ejecución de aplicaciones"

- Compatibilidad con Cloud Volumes ONTAP de NetApp como back-end de almacenamiento

  "Más información sobre Astra Control"

22 de noviembre de 2022

Nuevas funciones y soporte

- Compatibilidad con aplicaciones que abarcan varios espacios de nombres

  "Defina las aplicaciones"

- Soporte para incluir recursos de clúster en una definición de aplicación

"Defina las aplicaciones"

- Generación de informes de progreso mejorado para sus operaciones de backup, restauración y clonado

  "Supervisar tareas en ejecución"

- Compatibilidad con la gestión de clústeres que ya cuentan con una versión compatible de Astra Trident instalada

  "Empiece a gestionar los clústeres de Kubernetes desde Astra Control Service"

- Compatibilidad con la gestión de suscripciones de varios proveedores de cloud en una única cuenta de Astra Control Service

  "Gestionar las instancias de cloud"

- Compatibilidad con la adición de clústeres de Kubernetes autogestionados en entornos de cloud público a Astra Control Service

  "Empiece a gestionar los clústeres de Kubernetes desde Astra Control Service"

- La facturación del Servicio de control de Astra ahora se controla por espacio de nombres en lugar de por aplicación

  "Configurar facturación"

- Soporte para suscribirse a las ofertas basadas en términos del servicio Astra Control Service a través de AWS Marketplace

  "Configurar facturación"

Problemas y limitaciones conocidos

- "Problemas conocidos de esta versión"
- "Limitaciones conocidas de esta versión"

7 de septiembre de 2022

Esta versión incluye mejoras en la estabilidad y la resiliencia de la infraestructura del servicio Astra Control.

10 de agosto de 2022

Esta versión incluye las siguientes funciones y mejoras nuevas.

- Flujo de trabajo de gestión de aplicaciones mejorado los flujos de trabajo de gestión de aplicaciones mejorados proporcionan una mayor flexibilidad a la hora de definir aplicaciones gestionadas por Astra Control.

  "Gestionar aplicaciones"

- Compatibilidad con clústeres de Amazon Web Services Astra Control Service ahora puede gestionar las aplicaciones que se ejecutan en los clústeres alojados en Amazon Elastic Kubernetes Service. Puede configurar los clústeres para que usen Amazon Elastic Block Store o Amazon FSX para ONTAP de NetApp como back-end de almacenamiento.

"Configure Amazon Web Services"

- Enlaces de ejecución mejorados Además de enlaces de ejecución anteriores y posteriores a la instantánea, ahora puede configurar los siguientes tipos de enlaces de ejecución:

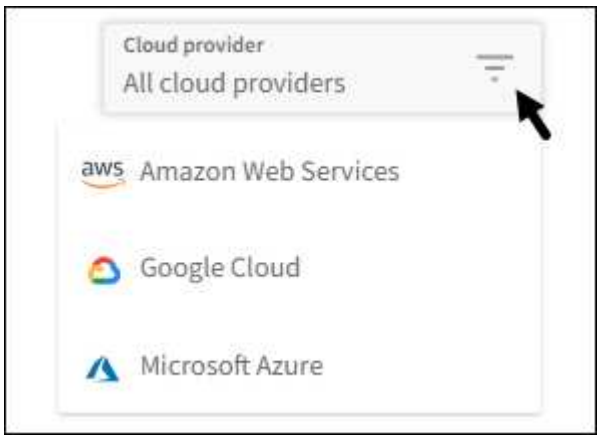
  - Previo al backup
  - Después del backup
  - Después de la restauración

  Entre otras mejoras, Astra Control ahora admite el uso de la misma secuencia de comandos para varios enlaces de ejecución.

  > En esta versión se han eliminado los enlaces de ejecución predeterminados previa y posterior a la copia Snapshot para aplicaciones específicas que ofrece NetApp. Si no proporciona sus propios enlaces de ejecución para instantáneas, Astra Control Service realizará instantáneas coherentes con los fallos a partir del 4 de agosto de 2022. Visite la "Repositorio de Verda GitHub de NetApp" para la ejecución de ejemplo de secuencias de comandos de enlace que puede modificar para ajustarse a su entorno.

  "Gestione los enlaces de ejecución de aplicaciones"

- El soporte para Azure Marketplace ahora puede inscribirse en Astra Control Service a través de Azure Marketplace.
- Selección de proveedor de cloud mientras lee la documentación de Astra Control Service, ahora puede seleccionar a su proveedor de cloud en la parte superior derecha de la página. La documentación solo será relevante para el proveedor de cloud que seleccione.



26 de abril de 2022

Esta versión incluye las siguientes funciones y mejoras nuevas.

- Namespace Control de acceso basado en funciones (RBAC) Astra Control Service ahora admite la asignación de restricciones de espacio de nombres a usuarios miembros o Viewer.

  "Control de acceso basado en roles (RBAC) del espacio de nombres"

- Compatibilidad de Azure Active Directory con Astra Control Service es compatible con clústeres AKS que utilizan Azure Active Directory para la autenticación y la gestión de identidades.

"Empiece a gestionar los clústeres de Kubernetes desde Astra Control Service"

- Compatibilidad con clústeres AKS privados ahora puede gestionar clústeres AKS que utilizan direcciones IP privadas.

  "Empiece a gestionar los clústeres de Kubernetes desde Astra Control Service"

- Retirada de la cuchara de Astra Control ahora puede retirar una cuchara del servicio Astra Control.

  "Retirar un cucharón"

14 de diciembre de 2021

Esta versión incluye las siguientes funciones y mejoras nuevas.

- Nuevas opciones de entorno de administración del almacenamiento
- Restauración de aplicaciones in situ puede restaurar una snapshot, un clon o un backup de una aplicación in situ restaurando el mismo clúster y espacio de nombres.

  "Restaurar aplicaciones"

- Eventos de secuencias de comandos con enlaces de ejecución Astra Control admite secuencias de comandos personalizadas que puede ejecutar antes o después de tomar una instantánea de una aplicación. Esto le permite realizar tareas como suspender transacciones de base de datos para que la instantánea de la aplicación de base de datos sea coherente.

  "Gestione los enlaces de ejecución de aplicaciones"

- Aplicaciones implementadas por el operador Astra Control admite algunas aplicaciones cuando se ponen en marcha con los operadores.

  "Inicie la gestión de aplicaciones"

- Los directores de servicio con ámbito de grupo de recursos Astra Control Service ahora son compatibles con los principales de servicio que utilizan un ámbito de grupo de recursos.

  "Cree un principal de servicio de Azure"

5 de agosto de 2021

Esta versión incluye las siguientes funciones y mejoras nuevas.

- Astra Control Center
  Astra Control ya está disponible en un nuevo modelo de puesta en marcha. *Astra Control Center* es un software autogestionado que se instala y opera en el centro de datos para poder gestionar la gestión del ciclo de vida de las aplicaciones de Kubernetes para clústeres de Kubernetes en las instalaciones.

  Para obtener más información, "Vaya a la documentación de Astra Control Center".

- Traiga su propio bucket, ahora puede gestionar los bloques que emplea Astra para backups y clones mediante la adición de bloques adicionales y el cambio del bloque predeterminado para los clústeres de Kubernetes de su proveedor de cloud.

  "Gestionar bloques"

2 de junio de 2021

Esta versión incluye correcciones de errores y las siguientes mejoras para la compatibilidad con Google Cloud.

- Compatibilidad con VPC compartidos ahora puede gestionar clústeres GKE en proyectos GCP con una configuración de red VPC compartida.
- El tamaño de volumen persistente para el tipo de servicio CVS Astra Control Service ahora crea volúmenes persistentes con un tamaño mínimo de 300 GIB cuando se usa el tipo de servicio CVS.

  "Descubra cómo el servicio Astra Control utiliza Cloud Volumes Service para Google Cloud como back-end de almacenamiento para volúmenes persistentes".

- La compatibilidad con el SO optimizado para contenedores del SO optimizado para contenedores ahora es compatible con los nodos de trabajo GKE. Esto es además de la compatibilidad con Ubuntu.

  "Obtenga más información sobre los requisitos del clúster GKE".

15 de abril de 2021

Esta versión incluye las siguientes funciones y mejoras nuevas.

- Compatibilidad con clústeres AKS Astra Control Service ahora puede gestionar aplicaciones que se ejecutan en un clúster Kubernetes gestionado en Azure Kubernetes Service (AKS).

  "Aprenda cómo empezar".

- API REST la API REST de Astra Control ya está disponible para su uso. La API se basa en tecnologías modernas y en las mejores prácticas actuales.

  "Aprenda a automatizar la gestión del ciclo de vida de los datos de aplicaciones con la API DE REST".

- Suscripción anual Astra Control Service ahora ofrece una *Premium Subscription*.

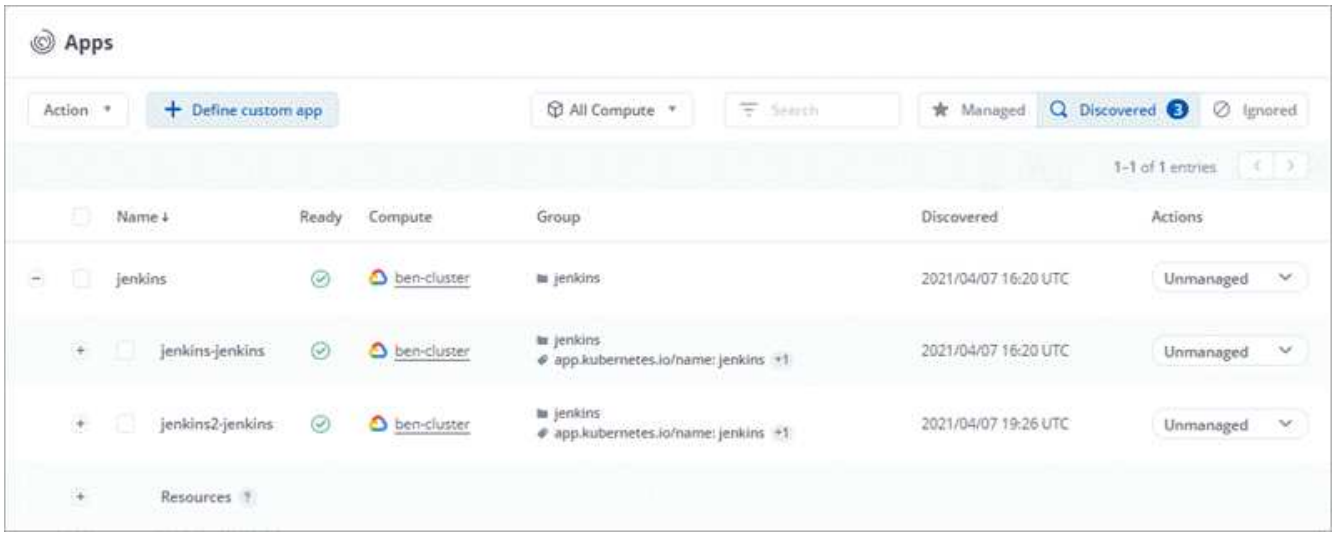
  Prepago a una tarifa con descuento con una suscripción anual que le permite gestionar hasta 10 aplicaciones por cada paquete de aplicaciones_. Póngase en contacto con el equipo de ventas de NetApp para adquirir tantos paquetes como sea necesario para su organización; por ejemplo, adquiera 3 paquetes para gestionar 30 aplicaciones de Astra Control Service.

  Si gestiona más aplicaciones de las permitidas en su suscripción anual, se le cobrará una tasa de exceso de 0.005 dólares por minuto, por aplicación (igual que Premium PAYGO).

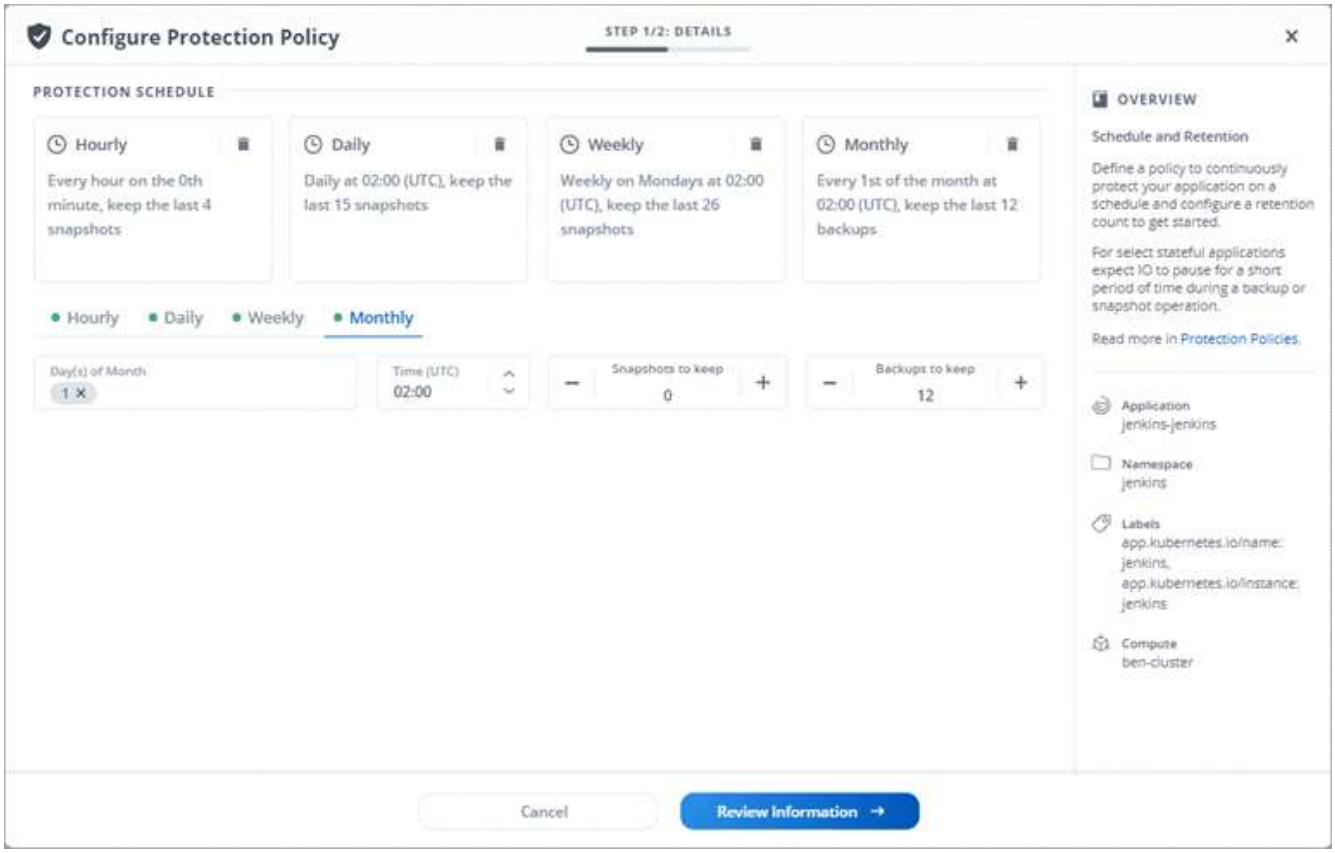
  "Más información sobre los precios del servicio Astra Control".

- Espacio de nombres y visualización de aplicaciones hemos mejorado la página aplicaciones descubiertas para mostrar mejor la jerarquía entre espacios de nombres y aplicaciones. Solo tiene que ampliar un espacio de nombres para ver las aplicaciones que contiene dicho espacio de nombres.

  "Más información sobre la gestión de aplicaciones".



- Mejoras en la interfaz de usuario los asistentes de protección de datos han sido mejorados para facilitar su uso. Por ejemplo, hemos refinado el Asistente para políticas de protección para ver más fácilmente el programa de protección cuando lo define.



- Mejoras en las actividades hemos facilitado la visualización de los detalles de las actividades de su cuenta de Astra Control.
  - Filtre la lista de actividades por aplicación gestionada, nivel de gravedad, usuario y intervalo de tiempo.
  - Descargue la actividad de su cuenta de Astra Control en un archivo CSV.
  - Vea las actividades directamente en la página Clusters o la página Apps después de seleccionar un clúster o una aplicación.

"Obtenga más información sobre cómo ver la actividad de su cuenta".

1 de marzo de 2021

Astra Control Service ahora es compatible con "Tipo de servicio *CVS*" Con Cloud Volumes Service para Google Cloud. Esto es además de ser compatible con el tipo de servicio *CVS-Performance*. A modo de recordatorio, Astra Control Service utiliza Cloud Volumes Service para Google Cloud como back-end de almacenamiento para sus volúmenes persistentes.

Esta mejora implica que el servicio Astra Control Service ahora puede gestionar los datos de aplicaciones para los clústeres de Kubernetes que se ejecutan en *any* "Región de Google Cloud en la que Cloud Volumes Service es compatible".

Si tiene la flexibilidad para elegir entre regiones de Google Cloud, puede elegir CVS o CVS-Performance, según sus requisitos de rendimiento. "Obtenga más información sobre cómo elegir un tipo de servicio".

25 de enero de 2021

Nos complace anunciar que Astra Control Service ya está disponible en general. Incorporamos muchos de los comentarios que recibimos de la versión beta e hicimos algunas mejoras notables.

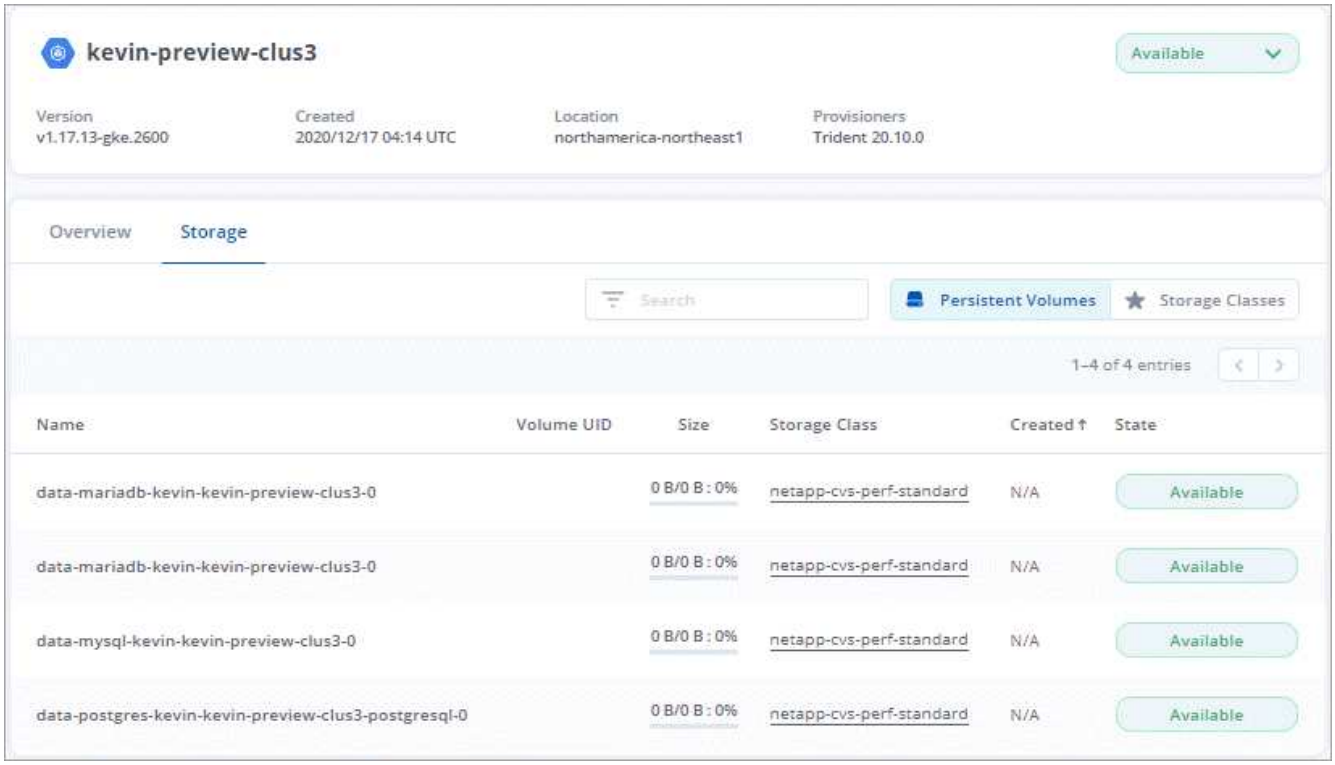
- La facturación está ahora disponible, lo que le permite pasar del Plan libre al Plan Premium. "Más información sobre facturación".
- Astra Control Service ahora crea volúmenes persistentes con un tamaño mínimo de 100 GIB cuando se usa el tipo de servicio CVS-Performance.
- Astra Control Service ahora puede descubrir aplicaciones más rápido.
- Ahora puede crear y eliminar cuentas por su cuenta.
- Hemos mejorado las notificaciones cuando Astra Control Service ya no puede acceder a un clúster de Kubernetes.

  Estas notificaciones son importantes porque Astra Control Service no puede gestionar aplicaciones para clústeres desconectados.

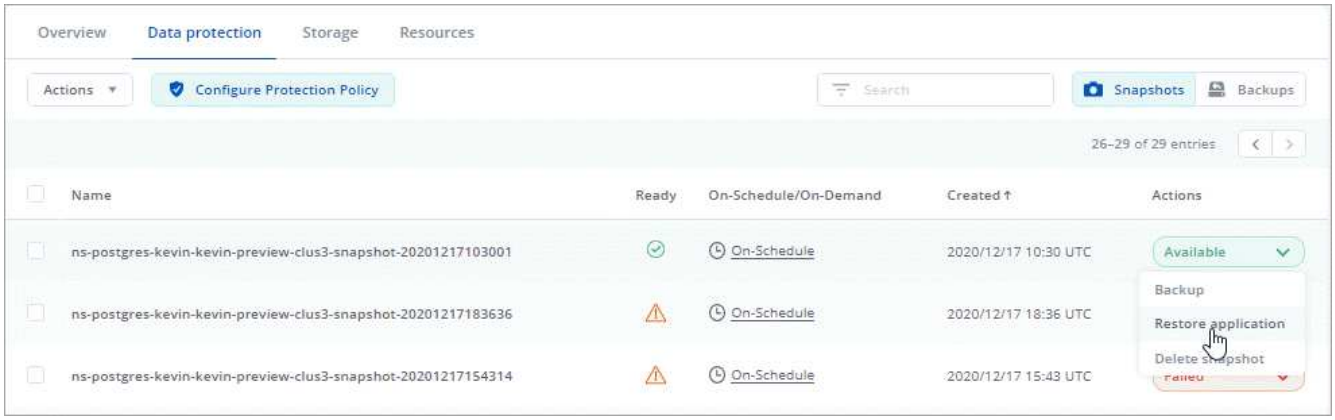
17 de diciembre de 2020 (actualización Beta)

Nos centramos principalmente en correcciones de errores para mejorar su experiencia, pero hemos realizado algunas otras mejoras significativas:

- Cuando se añade la primera tecnología Kubernetes a Astra Control Service, el almacén de objetos se crea ahora en la zona geográfica donde reside el clúster.
- Ahora hay detalles sobre los volúmenes persistentes disponibles cuando se ven detalles de almacenamiento en el nivel de computación.



- Hemos añadido una opción para restaurar una aplicación desde un snapshot o backup existente.



- Si elimina un clúster Kubernetes que Astra Control Service está gestionando, el clúster ahora aparece en el estado **eliminado**. A continuación, puede eliminar el clúster del servicio Astra Control Service.
- Ahora los propietarios de las cuentas pueden modificar los roles asignados a otros usuarios.
- Hemos añadido una sección para facturación, que se activará cuando Astra Control Service sea lanzado para General Availability (GA).

Problemas conocidos

Los problemas conocidos identifican problemas por los que el uso correcto de esta versión del producto puede resultar imposible.

Los siguientes problemas conocidos afectan a la versión actual:

Aplicaciones

- No se puede definir una aplicación en un espacio de nombres que se haya eliminado y vuelto a crear

Backup, restauración y clonado

- Los clones de aplicaciones producen un error al utilizar una versión específica de PostgreSQL
- Los backups de aplicaciones y las snapshots producen errores si la clase volumesnapshotse añade después de gestionar un clúster
- Las operaciones de restauración sin movimiento a las clases de almacenamiento económico ontap-nas fallan
- Puede producirse un error en la restauración desde un backup cuando se utiliza el cifrado en tránsito de Kerberos
- Los datos de backup permanecen en bloque tras la eliminación de bloques con política de retención vencida

Otros temas

- Las operaciones de gestión de datos de aplicaciones producen errores internos de servicio (500) cuando Astra Trident está sin conexión

No se puede definir una aplicación en un espacio de nombres que se haya eliminado y vuelto a crear

Si define una aplicación con un espacio de nombres, elimina el espacio de nombres y, a continuación, vuelve a instalar la aplicación en el mismo espacio de nombres, la operación falla con un código de error 409. Para definir la aplicación mediante el espacio de nombres recreado, elimine primero la instancia antigua de la aplicación.

Los clones de aplicaciones producen un error al utilizar una versión específica de PostgreSQL

Los clones de aplicaciones dentro del mismo clúster fallan constantemente con el gráfico BitNami PostgreSQL 11.5.0. Para clonar correctamente, utilice una versión anterior o posterior del gráfico.

Los backups de aplicaciones y las snapshots producen errores si la clase volumesnapshotse añade después de gestionar un clúster

En este escenario, se produce un error de interfaz de usuario 500 en los backups y las snapshots. Como solución alternativa, actualice la lista de aplicaciones.

Las operaciones de restauración sin movimiento a las clases de almacenamiento económico ontap-nas fallan

Si realiza una restauración sin movimiento de una aplicación (restaura la aplicación en su espacio de nombres original) y la clase de almacenamiento de la aplicación utiliza el `ontap-nas-economy` controlador, se puede producir un error en la operación de restauración si el directorio snapshot no está oculto. Antes de restaurar en el lugar, siga las instrucciones de "Habilite el backup y la restauración para las operaciones económicas de ontap-nas" para ocultar el directorio de instantáneas.

Puede producirse un error en la restauración desde un backup cuando se utiliza el cifrado en tránsito de Kerberos

Cuando se restaura una aplicación desde un backup a un back-end de almacenamiento que utiliza el cifrado

en tránsito de Kerberos, se puede producir un error en la operación de restauración. Este problema no afecta a la restauración de una copia Snapshot ni a la replicación de los datos de la aplicación mediante SnapMirror de NetApp.

> Cuando use el cifrado en tránsito de Kerberos con volúmenes NFSv4, asegúrese de que los volúmenes NFSv4 estén utilizando la configuración correcta. Consulte la sección Configuración de dominio de NetApp NFSv4 (página 13) del "Guía de mejoras y prácticas recomendadas de NetApp NFSv4".

Los datos de backup permanecen en bloque tras la eliminación de bloques con política de retención vencida

Si elimina el backup inmutable de una aplicación después de que la política de retención del bloque haya caducado, el backup se eliminará de Astra Control, pero no del bloque. Este problema se solucionará en una próxima versión.

Las operaciones de gestión de datos de aplicaciones producen errores internos de servicio (500) cuando Astra Trident está sin conexión

Si Astra Trident se desconecta (y se vuelve a conectar) y se producen 500 errores internos de servicio al intentar gestionar los datos de las aplicaciones, reinicie todos los nodos de Kubernetes del clúster de aplicaciones para restaurar la funcionalidad.

Limitaciones conocidas

Las limitaciones conocidas identifican plataformas, dispositivos o funciones que no son compatibles con esta versión del producto o cuya interoperabilidad con esta no es óptima. Revise estas limitaciones detenidamente.

Limitaciones generales

Las siguientes limitaciones afectan a la gestión de los clústeres de Kubernetes de Astra Control Service en cualquier puesta en marcha de Kubernetes compatible.

Las conexiones existentes a un pod Postgres provocan fallos

Cuando realice operaciones en pods Postgres, no debe conectarse directamente dentro del pod para utilizar el comando psql. Astra Control Service requiere un acceso psql para congelar y descongelar las bases de datos. Si existe una conexión preexistente, se producirá un error en la snapshot, el backup o el clon.

La página Actividad muestra hasta 100.000 eventos

La página Actividad de Astra Control puede mostrar hasta 100.000 eventos. Para ver todos los eventos registrados, recupere los eventos mediante "API REST de Astra Control".

Limitaciones en la administración de clústeres GKE

Las siguientes limitaciones se aplican a la gestión de los clústeres de Kubernetes en Google Kubernetes Engine (GKE).

Limitaciones en la gestión de aplicaciones

Las siguientes limitaciones afectan a la gestión de aplicaciones de Astra Control Service.

No es posible restaurar colectivamente varias aplicaciones que utilicen el mismo espacio de nombres para otro

Si gestiona varias aplicaciones que utilizan el mismo espacio de nombres (creando varias definiciones de aplicaciones en Astra Control), no podrá restaurar todas las aplicaciones en un espacio de nombres único diferente. Es necesario restaurar cada aplicación a su propio espacio de nombres independiente.

Astra Control no asigna automáticamente bloques predeterminados para las instancias de la nube

Astra Control no asigna automáticamente un bloque predeterminado para ninguna instancia de cloud. Debe establecer manualmente un bloque predeterminado para una instancia de cloud. Si no se ha establecido un bloque predeterminado, no se podrán realizar operaciones de clonado de aplicaciones entre dos clústeres.

No se admiten las operaciones de restauración in situ de las aplicaciones que utilizan un administrador de certificados

Esta versión de Astra Control Service no admite la restauración local de aplicaciones con gestores de certificados. Se admiten las operaciones de restauración en otro espacio de nombres y operaciones de clonado.

Se produce un error en los clones de aplicaciones después de poner en marcha una aplicación con una clase de almacenamiento establecida

Una vez que se implementa una aplicación con una clase de almacenamiento definida explícitamente (por ejemplo, `helm install …-set global.storageClass=netapp-cvs-perf-extreme`), los intentos posteriores de clonar la aplicación requieren que el clúster de destino tenga la clase de almacenamiento especificada originalmente. Se producirá un error al clonar una aplicación con una clase de almacenamiento definida explícitamente a un clúster que no tenga la misma clase de almacenamiento. No existen pasos de recuperación en este escenario.

Se puede producir un error en los clones de aplicaciones instaladas con operadores de referencia de paso

Astra Control admite las aplicaciones instaladas con operadores con ámbito de espacio de nombres. Estos operadores están diseñados generalmente con una arquitectura "pasada por valor" en lugar de "pasada por referencia". Las siguientes son algunas aplicaciones del operador que siguen estos patrones:

- "Apache K8ssandra"

> Para K8ssandra, se admiten operaciones de restauración in situ. Una operación de restauración a un nuevo espacio de nombres o clúster requiere que se apague la instancia original de la aplicación. Esto es para garantizar que la información del grupo de pares no conduzca a la comunicación entre instancias. No se admite la clonación de la aplicación.

- "Jenkins CI"
- "Clúster Percona XtraDB"

Tenga en cuenta que Astra Control puede no ser capaz de clonar a un operador diseñado con una arquitectura "de paso por referencia" (por ejemplo, el operador CockroachDB). Durante estos tipos de operaciones de clonado, el operador clonado intenta hacer referencia a los secretos de Kubernetes del

operador de origen a pesar de tener su propio secreto nuevo como parte del proceso de clonado. Es posible que se produzca un error en la operación de clonado porque Astra Control no conoce los secretos de Kubernetes en el operador de origen.

> Durante las operaciones de clonado, las aplicaciones que necesitan un recurso IngressClass o enlaces web para funcionar correctamente no deben tener esos recursos ya definidos en el clúster de destino.

Limitaciones de control de acceso basado en roles (RBAC)

Las siguientes limitaciones se aplican a la forma en que Astra Control limita el acceso de los usuarios a los recursos o capacidades.

Un usuario con restricciones de RBAC de espacio de nombres puede añadir y anular la gestión de un clúster

No se debe permitir que un usuario con restricciones de RBAC de espacio de nombres añada o anule la gestión de clústeres. Debido a una limitación actual, Astra no impide que estos usuarios desgestionen los clústeres.

Un usuario miembro con restricciones de espacio de nombres no puede acceder a las aplicaciones clonadas o restauradas hasta que un usuario Admin agregue el espacio de nombres a la restricción

Cualquiera `member` El usuario con limitaciones de RBAC por nombre/ID de espacio de nombres puede clonar o restaurar una aplicación en un espacio de nombres nuevo en el mismo clúster o en cualquier otro clúster de la cuenta de la organización. Sin embargo, el mismo usuario no puede acceder a la aplicación clonada o restaurada en el nuevo espacio de nombres. Una vez que una operación de clonado o restauración crea un nuevo espacio de nombres, el administrador/propietario de la cuenta puede editar el `member` cuenta de usuario y restricciones de función de actualización para que el usuario afectado conceda acceso al nuevo espacio de nombres.

Es posible que las copias de Snapshot fallen en clústeres de Kubernetes 1,25 o posteriores con ciertas versiones de controladoras Snapshot

Las snapshots de los clústeres de Kubernetes que ejecutan la versión 1,25 o posterior pueden fallar si la versión v1beta1 de las API del controlador de snapshots se instala en el clúster.

Como solución alternativa, haga lo siguiente al actualizar instalaciones existentes de Kubernetes 1,25 o posteriores:

1. Elimine cualquier CRD de Snapshot existente y cualquier controlador de instantánea existente.
2. "Desinstale Astra Trident".
3. "Instale los CRD de instantánea y el controlador de instantánea".
4. "Instala la versión más reciente de Astra Trident".
5. "Cree una instancia de VolumeSnapshotClass".

Manos a la obra

Más información sobre Astra Control

Astra Control es una solución de gestión del ciclo de vida de los datos de las aplicaciones de Kubernetes que simplifica las operaciones para aplicaciones con estado. Proteja, realice backups y migre cargas de trabajo de Kubernetes con facilidad, y cree instantáneamente clones de aplicaciones que funcionen.

Funciones

Astra Control ofrece funcionalidades cruciales para la gestión del ciclo de vida de los datos de las aplicaciones Kubernetes:

- Gestione automáticamente el almacenamiento persistente
- Crear copias Snapshot y backups bajo demanda que se tienen en cuenta las aplicaciones
- Automatice las operaciones de backup y Snapshot condicionadas por políticas
- Migre aplicaciones y datos de un clúster de Kubernetes a otro
- Replicar aplicaciones en un sistema remoto mediante la tecnología SnapMirror de NetApp (Astra Control Center)
- Clone aplicaciones de almacenamiento provisional a producción
- Visualizar el estado de la protección y el estado de la aplicación
- Trabaje con una interfaz de usuario web o una API para implementar sus flujos de trabajo de backup y migración

Modelos de puesta en marcha

Astra Control está disponible en dos modelos de implementación:

- **Astra Control Service**: Un servicio gestionado por NetApp que proporciona gestión de datos para aplicaciones de clústeres de Kubernetes en varios entornos de proveedores de cloud, así como clústeres de Kubernetes autogestionados.
- **Astra Control Center**: Software autogestionado que proporciona gestión de datos para aplicaciones de clústeres de Kubernetes que se ejecutan en su entorno local. Astra Control Center también se puede instalar en entornos de varios proveedores de cloud con un entorno de administración del almacenamiento Cloud Volumes ONTAP de NetApp.

	Servicio de control Astra	**Astra Control Center**
¿Cómo se ofrece?	Como un servicio cloud totalmente gestionado de NetApp	Como software que se puede descargar, instalar y gestionar
¿Dónde está alojado?	En un cloud público que elija NetApp	En su propio clúster de Kubernetes
¿Cómo se actualiza?	Gestionado por NetApp	Usted administra cualquier actualización

	Servicio de control Astra	Astra Control Center

¿Cuáles son las distribuciones de Kubernetes compatibles?	• * Proveedores en la nube*
	  ◦ Amazon Web Services
	  ▪ Amazon Elastic Kubernetes Service (EKS)
	  ◦ Google Cloud
	  ▪ Google Kubernetes Engine (GKE)
	  ◦ Microsoft Azure
	  ▪ Azure Kubernetes Service (AKS)
	• **Clusters autogestionados**
	  ◦ Kubernetes (ascendente)
	  ◦ Motor Kubernetes de rancher (RKE)
	  ◦ OpenShift Container Platform de Red Hat
	• * Clústeres locales*
	  ◦ Red Hat OpenShift Container Platform en las instalaciones
		• Azure Kubernetes Service en HCI de pila de Azure
		• Anthos de Google
		• Kubernetes (ascendente)
		• Motor Kubernetes de rancher (RKE)
		• OpenShift Container Platform de Red Hat

	Servicio de control Astra	Astra Control Center
¿Cuáles son los back-ends de almacenamiento compatibles?	• * Proveedores en la nube* ◦ Amazon Web Services ▪ Amazon EBS ▪ Amazon FSX para ONTAP de NetApp ▪ "Cloud Volumes ONTAP" ◦ Google Cloud ▪ Disco persistente de Google ▪ Cloud Volumes Service de NetApp ▪ "Cloud Volumes ONTAP" ◦ Microsoft Azure ▪ Discos gestionados de Azure ▪ Azure NetApp Files ▪ "Cloud Volumes ONTAP" • **Clusters autogestionados** ◦ Amazon EBS ◦ Discos gestionados de Azure ◦ Disco persistente de Google ◦ "Cloud Volumes ONTAP" ◦ NetApp MetroCluster ◦ "El Longhorn" • * Clústeres locales* ◦ NetApp MetroCluster ◦ Sistemas ONTAP AFF y FAS de NetApp ◦ ONTAP Select de NetApp ◦ "Cloud Volumes ONTAP" ◦ "El Longhorn"	• Sistemas ONTAP AFF y FAS de NetApp • ONTAP Select de NetApp • "Cloud Volumes ONTAP" • "El Longhorn"

Funcionamiento del servicio Astra Control

Astra Control Service es un servicio cloud gestionado por NetApp que siempre está activo y actualizado con las últimas funcionalidades. Utiliza varios componentes para habilitar la gestión del ciclo de vida de los datos de aplicaciones.

En un nivel superior, Astra Control Service funciona de esta manera:

- Para comenzar a trabajar con Astra Control Service, configure su proveedor de cloud y inscríbase para obtener una cuenta Astra.

+ ** para los clusters GKE, el servicio Astra Control utiliza "Cloud Volumes Service de NetApp para Google Cloud" O discos persistentes de Google como back-end de almacenamiento para sus volúmenes persistentes.

+ ** para clusters de AKS, el servicio de control de Astra utiliza "Azure NetApp Files" O Azure gestionó discos como back-end de almacenamiento para sus volúmenes persistentes.

+ ** para clústeres de Amazon EKS, el servicio Astra Control utiliza "Amazon Elastic Block Store" o. "Amazon FSX para ONTAP de NetApp" como back-end de almacenamiento para sus volúmenes persistentes.

- Agregue su primera tecnología Kubernetes al servicio Astra Control. A continuación, el servicio de control de Astra realiza lo siguiente:
  - Crea un almacén de objetos en su cuenta de proveedor de cloud, que es donde se almacenan las copias de backup.

+ en Azure, Astra Control Service también crea un grupo de recursos, una cuenta de almacenamiento y claves para el contenedor Blob.

- Crea un nuevo rol de administrador y una cuenta de servicio de Kubernetes en el clúster.
- Utiliza el nuevo rol de administrador para instalar el enlace../concepts/architecture#astra-control-components[Astra Control Provisioner] en el clúster y crear una o varias clases de almacenamiento.
- Si utilizas una oferta de almacenamiento de servicios en la nube de NetApp como back-end de almacenamiento, el servicio Astra Control utiliza el aprovisionador de control de Astra para aprovisionar volúmenes persistentes para tus aplicaciones. Si utiliza discos administrados de Amazon EBS o Azure como back-end de almacenamiento, deberá instalar un controlador CSI específico del proveedor. Se proporcionan instrucciones de instalación en "Configure Amazon Web Services" y.. "Configure Microsoft Azure con discos gestionados de Azure".
  - En este momento, puede definir aplicaciones del clúster. Se aprovisionan volúmenes persistentes en el back-end de almacenamiento mediante la nueva clase de almacenamiento predeterminada.
  - A continuación, utilice Astra Control Service para gestionar estas aplicaciones y empiece a crear copias Snapshot, copias de seguridad y clones.

El plan gratuito de Astra Control le permite gestionar hasta 10 espacios de nombres en su cuenta. Si desea gestionar más de 10 espacios de nombres, deberá configurar la facturación mediante la actualización del plan gratuito al plan Premium.

Cómo funciona Astra Control Center

Astra Control Center se ejecuta en forma local en su propia nube privada.

Astra Control Center admite los clústeres de Kubernetes con un tipo de almacenamiento configurado por el aprovisionador de Astra Control con un back-end de almacenamiento de ONTAP.

Astra Control Center está totalmente integrado en el ecosistema de AutoSupport y Active IQ para proporcionar a los usuarios y el soporte de NetApp información sobre solución de problemas y uso.

Puede probar Astra Control Center con una licencia de evaluación de 90 días. La versión de evaluación es compatible con las opciones de correo electrónico y comunidad. Además, tendrá acceso a los artículos de la base de conocimientos y a la documentación desde la consola de soporte del producto.

Para instalar y utilizar Astra Control Center, tendrá que estar seguro "requisitos".

En un nivel superior, Astra Control Center funciona de esta manera:

- Instala Astra Control Center en su entorno local. Obtenga más información sobre cómo "Instalar Astra Control Center".
- Puede realizar algunas tareas de configuración como las siguientes:
  - Configurar la licencia.
  - Añada el primer clúster.
  - Añada el back-end de almacenamiento que se detecta al añadir el clúster.
  - Agregue un bloque de almacenamiento de objetos que almacenará las copias de seguridad de la aplicación.

Obtenga más información sobre cómo "Configure Astra Control Center".

Puede añadir aplicaciones al clúster. O bien, si ya tiene algunas aplicaciones en el clúster que se están gestionando, puede utilizar Astra Control Center para gestionarlas. A continuación, utilice Astra Control Center para crear copias Snapshot, backups, clones y relaciones de replicación.

Si quiere más información

- "Documentación de la familia de productos Astra de NetApp"
- "Documentación de Astra Control Center"
- "Documentación de la API de Astra Control"
- "Documentación de Astra Trident"
- "Documentación de ONTAP"

Puestas en marcha de Kubernetes compatibles

Astra Control Service puede gestionar las aplicaciones que se ejecutan en un clúster de Kubernetes gestionado en Amazon Elastic Kubernetes Service (EKS) y los clústeres que gestiona por su cuenta.

Astra Control Service puede gestionar las aplicaciones que se ejecutan en un clúster de Kubernetes gestionado en Google Kubernetes Engine (GKE) y los clústeres que gestiona por su cuenta.

Astra Control Service puede gestionar las aplicaciones que se ejecutan en un clúster de Kubernetes gestionado en Azure Kubernetes Service (AKS) y clústeres que gestiona por su cuenta.

- "Descubra cómo configurar Amazon Web Services para Astra Control Service".
- "Descubra cómo configurar Google Cloud para Astra Control Service".
- "Descubra cómo configurar Microsoft Azure con Azure NetApp Files para el servicio Astra Control".
- "Descubra cómo configurar Microsoft Azure con los discos gestionados de Azure para el servicio Astra Control".
- "Descubra cómo preparar los clústeres autogestionados antes de agregarlos al servicio de control de Astra".

Inicio rápido del servicio Astra Control

Esta página ofrece una descripción general de alto nivel de los pasos que necesita

completar para empezar con Astra Control Service. Los vínculos de cada paso le llevan a una página que proporciona más detalles.

[Uno] Configure su proveedor de cloud

1. Google Cloud:
    - Revise los requisitos del clúster de Google Kubernetes Engine.
    - Compre Cloud Volumes Service para Google Cloud a través de Google Cloud Marketplace.
    - Habilite las API necesarias.
    - Cree una cuenta de servicio y una clave de cuenta de servicio.
    - Configure la agrupación de redes desde su VPC a Cloud Volumes Service para Google Cloud.

      "Más información acerca de los requisitos de Google Cloud".

2. Servicios web de Amazon:
    - Revise los requisitos del clúster de Amazon Web Services.
    - Cree una cuenta de Amazon.
    - Instale la CLI de Amazon Web Services.
    - Cree un usuario de IAM.
    - Cree y adjunte una directiva de permisos.
    - Guarde las credenciales del usuario de IAM.

      "Obtenga más información acerca de los requisitos de Amazon Web Services".

3. Azure de Microsoft:

    - Revise los requisitos del clúster de Azure Kubernetes Service para el back-end de almacenamiento que ha decidido usar.

      "Obtenga más información acerca de los requisitos de Microsoft Azure y Azure NetApp Files".

   "Obtenga más información acerca de los requisitos de disco gestionado de Microsoft Azure y Azure".

Si va a gestionar su propio clúster y no está alojado en un proveedor de cloud, revise los requisitos de los clústeres autogestionados.
"Obtenga más información sobre los requisitos de clúster autogestionados".

[Dos] Complete el registro de Astra Control

1. Cree un "BlueXP de NetApp" cuenta.
2. Especifica tu ID de correo electrónico de BlueXP de NetApp al crear tu cuenta de Astra Control "Desde la página de producto de Astra Control".

"Obtenga más información sobre el proceso de registro".

[Tres] Agregue clústeres a Astra Control

Después de iniciar sesión, seleccione **Agregar clúster** para comenzar a gestionar el clúster con Astra Control.

"Obtenga más información acerca de cómo añadir clústeres".

Configure su proveedor de cloud

Configure Amazon Web Services

Hay que realizar algunos pasos para preparar su proyecto de Amazon Web Services antes de poder gestionar los clústeres de Amazon Elastic Kubernetes Service (EKS) con Astra Control Service.

Inicio rápido para configurar Amazon Web Services

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

[Uno] Revise los requisitos del servicio Astra Control para Amazon Web Services

Compruebe que los clústeres estén en buen estado y que ejecuten una versión de Kubernetes compatible, que los nodos de trabajo estén en línea y que ejecuten Linux o Windows, etc. Obtenga más información sobre este paso.

[Dos] Cree una cuenta de Amazon

Si aún no tiene una cuenta de Amazon, debe crear una para poder utilizar EKS. Obtenga más información sobre este paso.

[Tres] Instale la CLI de Amazon Web Services

Instale la CLI de AWS para que pueda gestionar AWS desde la línea de comandos. Siga las instrucciones paso a paso.

[Cuatro] Opcional: Cree un usuario de IAM

Cree un usuario de Amazon Identity and Access Management (IAM). También puede omitir este paso y utilizar un usuario de IAM existente con el servicio Astra Control Service.

Lea las instrucciones paso a paso.

[Cinco] Cree y adjunte una directiva de permisos

Cree una directiva con los permisos necesarios para que Astra Control Service interactúe con su cuenta de AWS.

Lea las instrucciones paso a paso.

[Seis] Guarde las credenciales del usuario de IAM

Guarde las credenciales del usuario de IAM para poder importar las credenciales en Astra Control Service.

Lea las instrucciones paso a paso.

Requisitos del clúster de EKS

Un clúster de Kubernetes debe cumplir los siguientes requisitos para que pueda detectar y gestionar estos sistemas desde el servicio Astra Control Service.

La versión de Kubernetes

Un clúster de debe ejecutar una versión de Kubernetes en el rango de 1,25 a 1,28.

Tipo de imagen

El tipo de imagen para cada nodo de trabajo debe ser Linux.

Estado del clúster

Los clústeres deben ejecutarse en buen estado y tener al menos un nodo de trabajo en línea sin nodos de trabajo en estado con errores.

Aprovisionador de Astra Control

Se necesitan un aprovisionador de Astra Control y una controladora Snapshot externa para las operaciones con back-ends de almacenamiento. Para habilitar estas operaciones, haga lo siguiente:

1. "Instale los CRD de instantánea y el controlador de instantánea".
2. "Habilita el aprovisionador de Astra Control".
3. "Cree una instancia de VolumeSnapshotClass".

Controladores CSI para Amazon Elastic Block Store (EBS)

Si utiliza el back-end de almacenamiento de Amazon EBS, debe instalar el controlador Container Storage Interface (CSI) para EBS (no se instala automáticamente).

Consulte los pasos para obtener instrucciones sobre la instalación del controlador CSI.

Instale una instantánea externa

Si aún no lo ha hecho, "Instale los CRD de instantánea y el controlador de instantánea".

Instale el controlador CSI como complemento Amazon EKS

1. Cree el rol IAM del controlador Amazon EBS CSI para las cuentas de servicio. Siga las instrucciones "En la documentación de Amazon", Mediante los comandos de la CLI de AWS de las instrucciones.
2. Añada el complemento Amazon EBS CSI con el siguiente comando de la CLI de AWS, reemplazando la información entre paréntesis <> por valores específicos de su entorno. Sustituya <DRIVER_ROLE> por el nombre de la función de controlador EBS CSI que creó en el paso anterior:

```
aws eks create-addon \
  --cluster-name <CLUSTER_NAME> \
  --addon-name aws-ebs-csi-driver \
  --service-account-role-arn
arn:aws:iam::<ACCOUNT_ID>:role/<DRIVER_ROLE>
```

Configure la clase de almacenamiento EBS

1. Clonar el repositorio del controlador Amazon EBS CSI GitHub en su sistema.

```
git clone https://github.com/kubernetes-sigs/aws-ebs-csi-
driver.git
```

2. Desplácese al directorio de ejemplo de aprovisionamiento dinámico.

```
cd aws-ebs-csi-driver/examples/kubernetes/dynamic-provisioning/
```

3. Implemente la clase de almacenamiento ebs-sc y la reclamación de volumen persistente ebs-Claim desde el directorio manifest.

```
kubectl apply -f manifests/storageclass.yaml
kubectl apply -f manifests/claim.yaml
```

4. Describa la clase de almacenamiento ebs-sc.

```
kubectl describe storageclass ebs-sc
```

Debe ver el resultado que describe los atributos de la clase de almacenamiento.

Cree una cuenta de Amazon

Si aún no dispone de una cuenta de Amazon, debe crear una para activar la facturación para Amazon EKS.

Pasos

1. Vaya a la "Página de inicio de Amazon" , Seleccione **Iniciar sesión** en la parte superior derecha y seleccione **Iniciar aquí**.
2. Siga las indicaciones para crear una cuenta.

Instale la CLI de Amazon Web Services

Instale la CLI de AWS para que pueda gestionar recursos de AWS desde la línea de comandos.

Paso

1. Vaya a. "Introducción a la CLI de AWS" Y siga las instrucciones para instalar la CLI.

Opcional: Cree un usuario de IAM

Cree un usuario de IAM para que pueda utilizar y gestionar los recursos y servicios de AWS con mayor seguridad. También puede omitir este paso y utilizar un usuario de IAM existente con el servicio Astra Control Service.

Paso

1. Vaya a. "Creación de usuarios de IAM" Y siga las instrucciones para crear un usuario de IAM.

Cree y adjunte una directiva de permisos

Cree una directiva con los permisos necesarios para que Astra Control Service interactúe con su cuenta de AWS.

Pasos

1. Cree un nuevo archivo llamado `policy.json`.
2. Copie el siguiente contenido JSON en el archivo:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData",
                "fsx:DescribeVolumes",
                "ec2:DescribeRegions",
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:PutObject",
                "s3:GetObject",
                "iam:SimulatePrincipalPolicy",
                "s3:ListAllMyBuckets",
                "eks:DescribeCluster",
                "eks:ListNodegroups",
                "eks:DescribeNodegroup",
                "eks:ListClusters",
                "iam:GetUser",
                "s3:DeleteObject",
                "s3:DeleteBucket",
                "autoscaling:DescribeAutoScalingGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

3. Cree la política:

```
POLICY_ARN=$(aws iam create-policy  --policy-name <policy-name> --policy
-document file://policy.json  --query='Policy.Arn' --output=text)
```

4. Adjunte la política al usuario del IAM. Sustituya `<IAM-USER-NAME>` Con el nombre de usuario del usuario de IAM que ha creado o un usuario de IAM existente:

```
aws iam attach-user-policy --user-name <IAM-USER-NAME> --policy-arn
=$POLICY_ARN
```

Guarde las credenciales del usuario de IAM

Guarde las credenciales del usuario de IAM para que pueda conocer al usuario el Servicio de control de Astra.

Pasos

1. Descargue las credenciales. Sustituya `<IAM-USER-NAME>` Con el nombre de usuario del usuario de IAM que se desea utilizar:

```
aws iam create-access-key --user-name <IAM-USER-NAME> --output json >
credential.json
```

Resultado

La `credential.json` Se crea el archivo y puede importar las credenciales en Astra Control Service.

Configure Google Cloud

Hay que realizar algunos pasos para preparar su proyecto de Google Cloud antes de poder gestionar los clústeres de Google Kubernetes Engine con Astra Control Service.

> Si no empieza a utilizar Google Cloud Volumes Service para Google Cloud como back-end de almacenamiento pero tiene previsto utilizarlo más adelante, debería completar los pasos necesarios para configurar Google Cloud Volumes Service para Google Cloud ahora. La creación de una cuenta de servicio más adelante significa que puede perder el acceso a los bloques de almacenamiento existentes.

Inicio rápido para configurar Google Cloud

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

[Uno] Revise los requisitos del servicio Astra Control para Google Kubernetes Engine

Compruebe que el estado de los clústeres sea bueno y ejecute una versión de Kubernetes compatible, que los nodos de trabajador estén en línea y que ejecuten un tipo de imagen compatible, etc. Obtenga más información sobre este paso.

[Dos] (Opcional): Adquiera Cloud Volumes Service para Google Cloud

Si planea utilizar Cloud Volumes Service para Google Cloud como back-end de almacenamiento, vaya a la página Cloud Volumes Service de NetApp en Google Cloud Marketplace y seleccione Purchase. Obtenga más información sobre este paso.

[Tres] Habilite API en su proyecto de Google Cloud

Habilite las siguientes API de Google Cloud:

- Google Kubernetes Engine
- Almacenamiento en cloud
- API JSON para el almacenamiento en cloud

- Uso de servicios
- API de Cloud Resource Manager
- Cloud Volumes Service de NetApp
  - Necesario para Cloud Volumes Service para Google Cloud
  - Opcional (pero recomendado) para Google Persistent Disk
- API de gestión de consumidores de servicios
- API de redes de servicio
- API de gestión de servicios

Siga las instrucciones paso a paso.

[Cuatro] Cree una cuenta de servicio que tenga los permisos necesarios

Cree una cuenta de servicio de Google Cloud que tenga los siguientes permisos:

- Administrador de Kubernetes Engine
- Administrador de Cloud Volumes de NetApp
  - Necesario para Cloud Volumes Service para Google Cloud
  - Opcional (pero recomendado) para Google Persistent Disk
- Administrador de almacenamiento
- Visor del uso del servicio
- Visor de red de computación

Lea las instrucciones paso a paso.

[Cinco] Cree una clave de cuenta de servicio

Cree una clave para la cuenta de servicio y guarde el archivo de claves en una ubicación segura. Siga las instrucciones paso a paso.

[Seis] (Opcional): Configure la agrupación de redes para el VPC

Si tiene pensado utilizar Cloud Volumes Service para Google Cloud como back-end de almacenamiento, configure interconexión de redes entre su VPC y Cloud Volumes Service para Google Cloud. Siga las instrucciones paso a paso.

Requisitos del clúster GKE

Un clúster de Kubernetes debe cumplir los siguientes requisitos para que pueda detectar y gestionar estos sistemas desde el servicio Astra Control Service. Tenga en cuenta que algunos de estos requisitos solo son aplicables si planea utilizar Cloud Volumes Service para Google Cloud como back-end de almacenamiento.

La versión de Kubernetes

Un clúster de debe ejecutar una versión de Kubernetes en el rango de 1,26 a 1,28.

Tipo de imagen

El tipo de imagen para cada nodo de trabajo debe ser `COS_CONTAINERD`.

Estado del clúster

Los clústeres deben ejecutarse en buen estado y tener al menos un nodo de trabajo en línea sin nodos de trabajo en estado con errores.

Región de Google Cloud

Si piensa utilizar Cloud Volumes Service para Google Cloud como back-end de almacenamiento, los clústeres se deben ejecutar en un "Región de Google Cloud en la que es compatible Cloud Volumes Service para Google Cloud." Tenga en cuenta que Astra Control Service admite ambos tipos de servicios: CVS y CVS-Performance. Como práctica recomendada, debe elegir una región que sea compatible con Cloud Volumes Service para Google Cloud, incluso si no la utiliza como back-end de almacenamiento. Esto facilita el uso de Cloud Volumes Service para Google Cloud como back-end de almacenamiento futuro si cambian sus requisitos de rendimiento.

Redes

Si planea usar Cloud Volumes Service para Google Cloud como back-end de almacenamiento, el clúster debe residir en un VPC que tenga una relación entre iguales con Cloud Volumes Service para Google Cloud. Este paso se describe a continuación.

Clústeres privados

Si el clúster es privado, el "redes autorizadas" Debe permitir la dirección IP del servicio Astra Control:

52.188.218.166/32

Modo de funcionamiento para un clúster GKE

Debe usar el modo de funcionamiento estándar. El modo de piloto automático no se ha probado en este momento. "Obtenga más información sobre los modos de funcionamiento".

Pools de almacenamiento

Si usa NetApp Cloud Volumes Service como back-end de almacenamiento con el tipo de servicio CVS, debe configurar los pools de almacenamiento antes de poder aprovisionar volúmenes. Consulte "Tipo de servicio, clases de almacenamiento y tamaño VP para clústeres GKE" si quiere más información.

Opcional: Adquiera Cloud Volumes Service para Google Cloud

Astra Control Service puede utilizar Cloud Volumes Service para Google Cloud como back-end de almacenamiento para sus volúmenes persistentes. Si planea utilizar este servicio, debe adquirir Cloud Volumes Service para Google Cloud en Google Cloud Marketplace para permitir la facturación de volúmenes persistentes.

Paso

1. Vaya a la "Página de Cloud Volumes Service de NetApp" En Google Cloud Marketplace, seleccione **Compra** y siga las indicaciones.

   "Siga las instrucciones paso a paso de la documentación de Google Cloud para adquirir y activar el servicio".

Habilite API en su proyecto

Su proyecto necesita permisos para acceder a API específicas de Google Cloud. Las API se utilizan para interactuar con recursos de Google Cloud, como los clústeres de Google Kubernetes Engine (GKE) y el almacenamiento de Cloud Volumes Service de NetApp.

Paso

1. "Utilice la consola de Google Cloud o la interfaz de línea de comandos gcloud para habilitar las siguientes API":
    - Google Kubernetes Engine
    - Almacenamiento en cloud
    - API JSON para el almacenamiento en cloud
    - Uso de servicios
    - API de Cloud Resource Manager
    - NetApp Cloud Volumes Service (necesario para Cloud Volumes Service para Google Cloud)
    - API de gestión de consumidores de servicios
    - API de redes de servicio
    - API de gestión de servicios

En el siguiente vídeo se muestra cómo habilitar las API desde la consola de Google Cloud.

► https://docs.netapp.com/es-es/astra-control-service/media/get-started/video-enable-gcp-apis.mp4 *(video)*

Cree una cuenta de servicio

Astra Control Service utiliza una cuenta de servicio de Google Cloud para facilitar la gestión de datos de aplicaciones de Kubernetes en su nombre.

Pasos

1. Vaya a Google Cloud y. "cree una cuenta de servicio mediante la consola, el comando gcloud u otro método preferido".
2. Otorgue a la cuenta de servicio las siguientes funciones:
    - **Kubernetes Engine Admin**: Se utiliza para enumerar clústeres y crear acceso de administrador para administrar aplicaciones.
    - **NetApp Cloud Volumes Admin**: Se utiliza para gestionar el almacenamiento persistente para aplicaciones.
    - **Administrador de almacenamiento**: Se utiliza para gestionar bloques y objetos para copias de seguridad de aplicaciones.
    - **Visor de uso del servicio**: Se utiliza para comprobar si están habilitadas las API necesarias de Cloud Volumes Service para Google Cloud.
    - **Visor de red de computación**: Se utiliza para comprobar si el VPC de Kubernetes está permitido para llegar a Cloud Volumes Service para Google Cloud.

Si desea usar gcloud, puede seguir los pasos de la interfaz Astra Control. Seleccione **cuenta > credenciales > Agregar credenciales** y, a continuación, seleccione **instrucciones**.

Si desea utilizar la consola de Google Cloud, en el siguiente vídeo se muestra cómo crear la cuenta de servicio desde la consola.

► https://docs.netapp.com/es-es/astra-control-service/media/get-started/video-create-gcp-service-

account.mp4 *(video)*

Configure la cuenta de servicio para un VPC compartido

Para administrar clústeres GKE que residen en un proyecto, pero que usan un VPC de otro proyecto (un VPC compartido), entonces debe especificar la cuenta de servicio Astra como miembro del proyecto host con la función **Visor de red informática**.

Pasos

1. Desde la consola de Google Cloud, vaya a **IAM & Admin** y seleccione **Cuentas de servicio**.
2. Busque la cuenta de servicio de Astra que tiene "los permisos necesarios" y, a continuación, copie la dirección de correo electrónico.
3. Vaya al proyecto anfitrión y seleccione **IAM y Admin** > **IAM**.
4. Seleccione **Agregar** y agregue una entrada para la cuenta de servicio.
   a. **Nuevos miembros**: Introduzca la dirección de correo electrónico de la cuenta de servicio.
   b. **Rol**: Seleccione **Visor de redes de computación**.
   c. Seleccione **Guardar**.

Resultado

La adición de un clúster GKE mediante un VPC compartido funcionará por completo con Astra.

Cree una clave de cuenta de servicio

En lugar de proporcionar un nombre de usuario y una contraseña al Servicio de control de Astra, proporcionará una clave de cuenta de servicio al agregar su primer clúster. Astra Control Service utiliza la clave de cuenta de servicio para establecer la identidad de la cuenta de servicio que acaba de configurar.

La clave de cuenta de servicio es texto sin formato almacenado en el formato JavaScript Object Notation (JSON). Contiene información sobre los recursos de GCP a los que tiene permiso para acceder.

Solo puede ver o descargar el archivo JSON cuando crea la clave. Sin embargo, puede crear una nueva clave en cualquier momento.

Pasos

1. Vaya a Google Cloud y. "cree una clave de cuenta de servicio mediante la consola, el comando gcloud u otro método preferido".
2. Cuando se le solicite, guarde el archivo de claves de la cuenta de servicio en una ubicación segura.

En el siguiente vídeo se muestra cómo crear la clave de cuenta de servicio desde la consola de Google Cloud.

► https://docs.netapp.com/es-es/astra-control-service/media/get-started/video-create-gcp-service-account-

key.mp4 *(video)*

Opcional: Configure la agrupación de redes para el VPC

Si piensa utilizar Cloud Volumes Service para Google Cloud como servicio de back-end de almacenamiento, el paso final es configurar una agrupación de redes entre su VPC y Cloud Volumes Service para Google Cloud.

La forma más sencilla de configurar Network peering es obtener los comandos gcloud directamente de Cloud Volumes Service. Los comandos se encuentran disponibles en Cloud Volumes Service al crear un nuevo sistema de archivos.

Pasos

1. "Ve a los mapas de regiones globales de NetApp BlueXP" E identifique el tipo de servicio que usará en la región de Google Cloud en la que resida su clúster.

   Cloud Volumes Service ofrece dos tipos de servicios: CVS y CVS-Performance. "Obtenga más información sobre estos tipos de servicio".

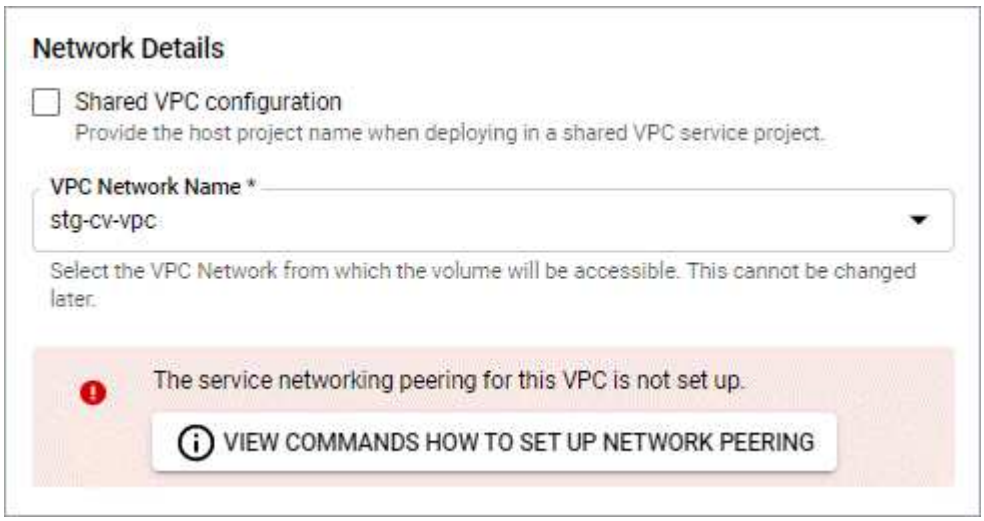
2. "Vaya a Cloud Volumes en Google Cloud Platform".
3. En la página **Volumes**, seleccione **Crear**.
4. En **Tipo de servicio**, seleccione **CVS** o **CVS-Performance**.

   Debe elegir el tipo de servicio correcto para su región de Google Cloud. Este es el tipo de servicio que ha identificado en el paso 1. Después de seleccionar un tipo de servicio, la lista de regiones de la página se actualiza con las regiones en las que se admite ese tipo de servicio.

   Después de este paso, solo tendrá que introducir la información de red para obtener los comandos.

5. En **Región**, seleccione su región y zona.
6. En **Detalles de red**, seleccione su VPC.

   Si no ha configurado la conexión de red, verá la siguiente notificación:



7. Seleccione el botón para ver los comandos de configuración de conexión de red.
8. Copie los comandos y ejecútelos en Cloud Shell.

   Para obtener más detalles sobre el uso de estos comandos, consulte "Inicio rápido de Cloud Volumes

Service para GCP".

"Obtenga más información sobre cómo configurar el acceso a los servicios privados y la configuración de la conexión a redes".

9. Una vez que haya terminado, puede seleccionar cancelar en la página **Crear sistema de archivos**.

   Comenzamos a crear este volumen sólo para obtener los comandos de conexión en red.

Configure Microsoft Azure con Azure NetApp Files

Es necesario realizar algunos pasos para preparar su suscripción a Microsoft Azure antes de poder gestionar los clústeres de Azure Kubernetes Service con Astra Control Service. Siga estas instrucciones si tiene pensado utilizar Azure NetApp Files como back-end de almacenamiento.

Inicio rápido para configurar Azure

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

[Uno] Revise los requisitos del servicio Astra Control para Azure Kubernetes Service

Compruebe que el estado de los clústeres sea bueno y ejecute una versión compatible de Kubernetes, que los pools de nodos estén en línea y que ejecuten Linux, etc. Obtenga más información sobre este paso.

[Dos] Regístrese para Microsoft Azure

Cree una cuenta de Microsoft Azure. Obtenga más información sobre este paso.

[Tres] Regístrese para Azure NetApp Files

Registre el proveedor de recursos de NetApp. Obtenga más información sobre este paso.

[Cuatro] Cree una cuenta de NetApp

Vaya a Azure NetApp Files en el portal de Azure y cree una cuenta de NetApp. Obtenga más información sobre este paso.

[Cinco] Configure pools de capacidad

Configure uno o varios pools de capacidad para los volúmenes persistentes. Obtenga más información sobre este paso.

[Seis] Delegar una subred en Azure NetApp Files

Delegue una subred en Azure NetApp Files para que el servicio de control de Astra pueda crear volúmenes persistentes en esa subred. Obtenga más información sobre este paso.

[Siete] Cree un principal de servicio de Azure

Cree una entidad de servicio de Azure con la función Colaborador. Obtenga más información sobre este paso.

[Ocho] Opcional: Configurar la redundancia para bloques de backup de Azure

De forma predeterminada, los bloques Astra Control Service utilizan para almacenar las copias de seguridad de Azure Kubernetes Service utilizan la opción de redundancia almacenamiento redundante local (LRS). Como paso opcional, puede configurar un nivel de redundancia más duradero para bloques de Azure. Obtenga más información sobre este paso.

Requisitos del clúster de Azure Kubernetes Service

Un clúster de Kubernetes debe cumplir los siguientes requisitos para que pueda detectar y gestionar estos sistemas desde el servicio Astra Control Service.

La versión de Kubernetes

Los clústeres deben ejecutar Kubernetes, de la versión 1,26 a la 1,28.

Tipo de imagen

El tipo de imagen para todos los pools de nodos debe ser Linux.

Estado del clúster

Los clústeres deben ejecutarse en buen estado y tener al menos un nodo de trabajo en línea sin nodos de trabajo en estado con errores.

Región de Azure

Los clústeres deben residir en una región donde Azure NetApp Files esté disponible. "Consulte los productos de Azure por región".

Suscripción

Los clústeres deben residir en una suscripción en la que Azure NetApp Files esté habilitado. Podrá elegir una suscripción cuando lo desee Regístrese para Azure NetApp Files.

Neta virtual

Considere los siguientes requisitos de vnet:

- Los clústeres deben residir en una red virtual que tenga acceso directo a una subred delegada de Azure NetApp Files. Aprenda a configurar una subred delegada.
- Si sus clústeres de Kubernetes están en una vnet con una relación entre iguales a la subred delegada de Azure NetApp Files que se encuentra en otra vnet, ambos lados de la conexión de paridad deben estar en línea.
- Tenga en cuenta que el límite predeterminado para el número de IP utilizadas en un vnet (incluidos los VNets de conexión inmediata) con Azure NetApp Files es 1,000. "Ver los límites de recursos de Azure NetApp Files".

  Si está cerca del límite, tiene dos opciones:

  - Puede hacerlo "enviar una solicitud de aumento de límite". Si necesita ayuda, póngase en contacto con su representante de NetApp.
  - Al crear un nuevo clúster de Amazon Kubernetes Service (AKS), especifique una nueva red para el clúster. Una vez creada la nueva red, aprovisione una nueva subred y delegue la subred a Azure NetApp Files.

Regístrese para Microsoft Azure

Si no tiene una cuenta de Microsoft Azure, comience registrándose en Microsoft Azure.

Pasos

1. Vaya a la "Página de suscripción a Azure" Para suscribirse al servicio de Azure.
2. Seleccione un plan y siga las instrucciones para completar la suscripción.

Regístrese para Azure NetApp Files

Obtenga acceso a Azure NetApp Files registrando el proveedor de recursos de NetApp.

Pasos

1. Inicie sesión en el portal de Azure.
2. "Siga la documentación de Azure NetApp Files para registrar el proveedor de recursos de NetApp".

Cree una cuenta de NetApp

Cree una cuenta de NetApp en Azure NetApp Files.

Paso

1. "Siga la documentación de Azure NetApp Files para crear una cuenta de NetApp desde el portal de Azure".

Configure un pool de capacidad

Se requieren uno o más pools de capacidad para que Astra Control Service pueda aprovisionar volúmenes persistentes en un pool de capacidad. Astra Control Service no crea pools de capacidad para usted.

Tenga en cuenta lo siguiente al configurar pools de capacidad para sus aplicaciones de Kubernetes:

- Los pools de capacidad deben crearse en la misma región de Azure en la que los clústeres de AKS se gestionarán con Astra Control Service.
- Un pool de capacidad puede tener un nivel de servicio Ultra, Premium o estándar. Cada uno de estos niveles de servicio está diseñado para satisfacer distintas necesidades de rendimiento. El servicio Astra Control es compatible con las tres.

  Es necesario configurar un pool de capacidad para cada nivel de servicio que se desea usar con los clústeres de Kubernetes.

  "Obtenga más información acerca de los niveles de servicio de Azure NetApp Files".

- Antes de crear un pool de capacidad para las aplicaciones que pretenda proteger con Astra Control Service, elija el rendimiento y la capacidad necesarios para esas aplicaciones.

  El aprovisionamiento de la cantidad adecuada de capacidad garantiza que los usuarios puedan crear volúmenes persistentes a medida que sean necesarios. Si la capacidad no está disponible, no se pueden aprovisionar los volúmenes persistentes.

- Un pool de capacidad de Azure NetApp Files puede usar el tipo de calidad de servicio manual o automática. Astra Control Service admite pools de capacidad de QoS automática. No se admiten pools de capacidad de calidad de servicio manual.

Paso

1. "Siga la documentación de Azure NetApp Files para configurar un pool de capacidad de calidad de servicio automática".

Delegar una subred en Azure NetApp Files

Debe delegar una subred en Azure NetApp Files para que el Servicio de control Astra pueda crear volúmenes persistentes en esa subred. Tenga en cuenta que Azure NetApp Files permite tener sólo una subred delegada en un vnet.

Si utiliza VNets con una relación entre iguales, ambos lados de la conexión entre iguales deben estar en línea: El vnet donde residen sus clústeres de Kubernetes y el vnet que tiene la subred delegada de Azure NetApp Files.

Paso

1. "Siga la documentación de Azure NetApp Files para delegar una subred en Azure NetApp Files".

Después de terminar

Espere unos 10 minutos antes de detectar el clúster que se ejecuta en la subred delegada.

Cree un principal de servicio de Azure

Astra Control Service requiere una entidad de servicio de Azure que tenga asignada la función Contributor. Astra Control Service utiliza este servicio principal para facilitar la gestión de los datos de aplicaciones de Kubernetes en su nombre.

Un principal de servicio es una identidad creada específicamente para su uso con aplicaciones, servicios y herramientas. La asignación de un rol al director de servicio restringe el acceso a recursos específicos de Azure.

Siga los pasos que se indican a continuación para crear un principal de servicio con la CLI de Azure. Deberá guardar el resultado en un archivo JSON y proporcionarlo al servicio de control de Astra más adelante. "Consulte la documentación de Azure para obtener más detalles sobre el uso de la CLI".

En los pasos siguientes se asume que tiene permiso para crear un principal de servicio y que tiene instalado el SDK de Microsoft Azure (comando az) en su equipo.

Requisitos

- El principal de servicio debe utilizar autenticación regular. No se admiten certificados.
- El director de servicio debe tener acceso a su suscripción de Azure a Contributor o propietario.
- La suscripción o el grupo de recursos que elija para Scope debe contener los clústeres de AKS y su cuenta de Azure NetApp Files.

Pasos

1. Identifique la suscripción y el ID de inquilino en los que residen los clústeres de AKS (estos son los clústeres que desea gestionar en Astra Control Service).

   ```
   az configure --list-defaults
   az account list --output table
   ```

2. Realice una de las siguientes acciones, en función de si utiliza una suscripción completa o un grupo de

recursos:

- Cree el principal de servicio, asigne la función Colaborador y especifique el ámbito de toda la suscripción donde residen los clústeres.

```
az ad sp create-for-rbac --name service-principal-name --role
contributor --scopes /subscriptions/SUBSCRIPTION-ID
```

- Cree el principal de servicio, asigne la función Colaborador y especifique el grupo de recursos donde residen los clústeres.

```
az ad sp create-for-rbac --name service-principal-name --role
contributor --scopes /subscriptions/SUBSCRIPTION-
ID/resourceGroups/RESOURCE-GROUP-ID
```

3. Almacene la salida de la CLI de Azure resultante como archivo JSON.

   Tendrá que proporcionar este archivo para que Astra Control Service pueda descubrir sus clústeres de AKS y gestionar las operaciones de gestión de datos de Kubernetes. "Obtenga más información sobre la gestión de credenciales en Astra Control Service".

4. Opcional: Agregue el ID de suscripción al archivo JSON para que Astra Control Service rellene automáticamente el ID cuando seleccione el archivo.

   De lo contrario, deberá introducir el identificador de suscripción en Astra Control Service cuando se le solicite.

   ejemplo

```
{
  "appId": "0db3929a-bfb0-4c93-baee-aaf8",
  "displayName": "sp-example-dev-sandbox",
  "name": "http://sp-example-dev-sandbox",
  "password": "mypassword",
  "tenant": "011cdf6c-7512-4805-aaf8-7721afd8ca37",
  "subscriptionId": "99ce999a-8c99-99d9-a9d9-99cce99f99ad"
}
```

5. Opcional: Pruebe el director de servicio. Elija entre los siguientes comandos de ejemplo según el ámbito que utilice su principal de servicio.

Alcance de la suscripción

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az group list --subscription SUBSCRIPTION-ID
az aks list --subscription SUBSCRIPTION-ID
az storage container list --account-name STORAGE-ACCOUNT-NAME
```

Ámbito del grupo de recursos

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az aks list --subscription SUBSCRIPTION-ID --resource-group RESOURCE-
GROUP-ID
```

Opcional: Configurar la redundancia para bloques de backup de Azure

Puede configurar un nivel de redundancia más duradero para bloques de backup de Azure. De forma predeterminada, los bloques Astra Control Service utilizan para almacenar las copias de seguridad de Azure Kubernetes Service utilizan la opción de redundancia almacenamiento redundante local (LRS). Para utilizar una opción de redundancia más duradera para bloques de Azure, debe hacer lo siguiente:

Pasos

1. Cree una cuenta de almacenamiento de Azure que utilice el nivel de redundancia necesario "estas instrucciones".
2. Cree un contenedor de Azure en la nueva cuenta de almacenamiento con "estas instrucciones".
3. Agregue el contenedor como cucharón al servicio de control Astra. Consulte "Añadir un bloque más".
4. (Opcional) para utilizar el bloque recién creado como bloque predeterminado para los backups de Azure, establezca esta opción como el bloque predeterminado para Azure. Consulte "Cambiar el bloque predeterminado".

Configure Microsoft Azure con discos gestionados de Azure

Es necesario realizar algunos pasos para preparar su suscripción a Microsoft Azure antes de poder gestionar los clústeres de Azure Kubernetes Service con Astra Control Service. Siga estas instrucciones si tiene pensado utilizar discos gestionados de Azure como back-end de almacenamiento.

Inicio rápido para configurar Azure

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

[Uno] Revise los requisitos del servicio Astra Control para Azure Kubernetes Service

Compruebe que el estado de los clústeres sea bueno y ejecute una versión compatible de Kubernetes, que los pools de nodos estén en línea y que ejecuten Linux, etc. Obtenga más información sobre este paso.

[Dos] Regístrese para Microsoft Azure

Cree una cuenta de Microsoft Azure. Obtenga más información sobre este paso.

[Tres] Cree un principal de servicio de Azure

Cree una entidad de servicio de Azure con la función Colaborador. Obtenga más información sobre este paso.

[Cuatro] Configure los detalles del controlador de la interfaz de almacenamiento del contenedor (CSI)

Necesita configurar su suscripción a Azure y el clúster para que funcionen con los controladores CSI. Obtenga más información sobre este paso.

[Cinco] Opcional: Configurar la redundancia para bloques de backup de Azure

De forma predeterminada, los bloques Astra Control Service utilizan para almacenar las copias de seguridad de Azure Kubernetes Service utilizan la opción de redundancia almacenamiento redundante local (LRS). Como paso opcional, puede configurar un nivel de redundancia más duradero para bloques de Azure. Obtenga más información sobre este paso.

Requisitos del clúster de Azure Kubernetes Service

Un clúster de Kubernetes debe cumplir los siguientes requisitos para que pueda detectar y gestionar estos sistemas desde el servicio Astra Control Service.

La versión de Kubernetes

Los clústeres deben ejecutar Kubernetes, de la versión 1,26 a la 1,28.

Tipo de imagen

El tipo de imagen para todos los pools de nodos debe ser Linux.

Estado del clúster

Los clústeres deben ejecutarse en buen estado y tener al menos un nodo de trabajo en línea sin nodos de trabajo en estado con errores.

Región de Azure

Como práctica recomendada, debe elegir una región que sea compatible con Azure NetApp Files, incluso si no la utiliza como back-end de almacenamiento. Esto facilita el uso de Azure NetApp Files como back-end de almacenamiento en el futuro si sus requisitos de rendimiento cambian. "Consulte los productos de Azure por región".

Controladores CSI

Los clústeres deben tener instalados los controladores CSI adecuados.

Regístrese para Microsoft Azure

Si no tiene una cuenta de Microsoft Azure, comience registrándose en Microsoft Azure.

Pasos

1. Vaya a la "Página de suscripción a Azure" Para suscribirse al servicio de Azure.
2. Seleccione un plan y siga las instrucciones para completar la suscripción.

Cree un principal de servicio de Azure

Astra Control Service requiere una entidad de servicio de Azure que tenga asignada la función Contributor. Astra Control Service utiliza este servicio principal para facilitar la gestión de los datos de aplicaciones de Kubernetes en su nombre.

Un principal de servicio es una identidad creada específicamente para su uso con aplicaciones, servicios y herramientas. La asignación de un rol al director de servicio restringe el acceso a recursos específicos de Azure.

Siga los pasos que se indican a continuación para crear un principal de servicio con la CLI de Azure. Deberá guardar el resultado en un archivo JSON y proporcionarlo al servicio de control de Astra más adelante. "Consulte la documentación de Azure para obtener más detalles sobre el uso de la CLI".

En los pasos siguientes se asume que tiene permiso para crear un principal de servicio y que tiene instalado el SDK de Microsoft Azure (comando az) en su equipo.

Requisitos

- El principal de servicio debe utilizar autenticación regular. No se admiten certificados.
- El director de servicio debe tener acceso a su suscripción de Azure a Contributor o propietario.
- La suscripción o el grupo de recursos que elija para Scope debe contener los clústeres de AKS y su cuenta de Azure NetApp Files.

Pasos

1. Identifique la suscripción y el ID de inquilino en los que residen los clústeres de AKS (estos son los clústeres que desea gestionar en Astra Control Service).

   ```
   az configure --list-defaults
   az account list --output table
   ```

2. Realice una de las siguientes acciones, en función de si utiliza una suscripción completa o un grupo de recursos:
   - Cree el principal de servicio, asigne la función Colaborador y especifique el ámbito de toda la suscripción donde residen los clústeres.

     ```
     az ad sp create-for-rbac --name service-principal-name --role
     contributor --scopes /subscriptions/SUBSCRIPTION-ID
     ```

   - Cree el principal de servicio, asigne la función Colaborador y especifique el grupo de recursos donde residen los clústeres.

     ```
     az ad sp create-for-rbac --name service-principal-name --role
     contributor --scopes /subscriptions/SUBSCRIPTION-
     ID/resourceGroups/RESOURCE-GROUP-ID
     ```

3. Almacene la salida de la CLI de Azure resultante como archivo JSON.

Tendrá que proporcionar este archivo para que Astra Control Service pueda descubrir sus clústeres de AKS y gestionar las operaciones de gestión de datos de Kubernetes. "Obtenga más información sobre la gestión de credenciales en Astra Control Service".

4. Opcional: Agregue el ID de suscripción al archivo JSON para que Astra Control Service rellene automáticamente el ID cuando seleccione el archivo.

   De lo contrario, deberá introducir el identificador de suscripción en Astra Control Service cuando se le solicite.

   ejemplo

```
{
  "appId": "0db3929a-bfb0-4c93-baee-aaf8",
  "displayName": "sp-example-dev-sandbox",
  "name": "http://sp-example-dev-sandbox",
  "password": "mypassword",
  "tenant": "011cdf6c-7512-4805-aaf8-7721afd8ca37",
  "subscriptionId": "99ce999a-8c99-99d9-a9d9-99cce99f99ad"
}
```

5. Opcional: Pruebe el director de servicio. Elija entre los siguientes comandos de ejemplo según el ámbito que utilice su principal de servicio.

   Alcance de la suscripción

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az group list --subscription SUBSCRIPTION-ID
az aks list --subscription SUBSCRIPTION-ID
az storage container list --account-name STORAGE-ACCOUNT-NAME
```

   Ámbito del grupo de recursos

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az aks list --subscription SUBSCRIPTION-ID --resource-group RESOURCE-
GROUP-ID
```

Configure los detalles del controlador de la interfaz de almacenamiento del contenedor (CSI)

Para utilizar discos administrados de Azure con Astra Control Service, tendrá que instalar los controladores CSI necesarios.

Active la función de controlador CSI en su suscripción a Azure

Antes de instalar los controladores CSI, debe activar la función de controlador CSI en su suscripción a Azure.

Pasos

1. Abra la interfaz de línea de comandos de Azure.
2. Ejecute el siguiente comando para registrar el controlador:

```
az feature register --namespace "Microsoft.ContainerService" --name
"EnableAzureDiskFileCSIDriver"
```

3. Ejecute el siguiente comando para garantizar que el cambio se propaga:

```
az provider register -n Microsoft.ContainerService
```

Debería ver una salida similar a la siguiente:

```
{
"id": "/subscriptions/b200155f-001a-43be-87be-
3edde83acef4/providers/Microsoft.Features/providers/Microsoft.ContainerSer
vice/features/EnableAzureDiskFileCSIDriver",
"name": "Microsoft.ContainerService/EnableAzureDiskFileCSIDriver",
"properties": {
   "state": "Registering"
},
"type": "Microsoft.Features/providers/features"
}
```

Instale los controladores CSI de disco gestionado de Azure en su clúster de Azure Kubernetes Service

Puede instalar los controladores de Azure CSI para completar la preparación.

Paso

1. Vaya a. "La documentación del controlador Microsoft CSI".
2. Siga las instrucciones para instalar los controladores CSI necesarios.

Opcional: Configurar la redundancia para bloques de backup de Azure

Puede configurar un nivel de redundancia más duradero para bloques de backup de Azure. De forma predeterminada, los bloques Astra Control Service utilizan para almacenar las copias de seguridad de Azure Kubernetes Service utilizan la opción de redundancia almacenamiento redundante local (LRS). Para utilizar una opción de redundancia más duradera para bloques de Azure, debe hacer lo siguiente:

Pasos

1. Cree una cuenta de almacenamiento de Azure que utilice el nivel de redundancia necesario "estas instrucciones".
2. Cree un contenedor de Azure en la nueva cuenta de almacenamiento con "estas instrucciones".
3. Agregue el contenedor como cucharón al servicio de control Astra. Consulte "Añadir un bloque más".

4. (Opcional) para utilizar el bloque recién creado como bloque predeterminado para los backups de Azure, establezca esta opción como el bloque predeterminado para Azure. Consulte "Cambiar el bloque predeterminado".

Regístrese para obtener una cuenta de Astra Control Service

Para utilizar el servicio de control de Astra, necesitas una cuenta del servicio de control de Astra que esté asociada con tu cuenta de BlueXP de NetApp. Completa el proceso de registro del servicio Astra Control y, si aún no tienes una cuenta de BlueXP, regístrate en BlueXP para acceder a Astra Control Service.

Regístrese para obtener una cuenta de Astra Control

Antes de iniciar sesión en Astra Control Service, necesita completar un proceso de registro para obtener una cuenta de Astra Control Service.

Cuando utilice Astra Control Service, gestionará sus aplicaciones desde una cuenta. Una cuenta incluye usuarios que pueden ver y gestionar las aplicaciones de la cuenta, así como los detalles de facturación.

Pasos

1. "Ve a la página de Astra Control en BlueXP".
2. Selecciona **Regístrate para el plan gratuito**.
3. Proporcione la información necesaria en el formulario.

   Algunas cosas importantes que debe tener en cuenta al rellenar el formulario:

   - El nombre y la dirección de su empresa deben ser precisos porque los verificamos para cumplir los requisitos de Global Trade Compliance.
   - * Nombre de cuenta Astra* es el nombre de la cuenta de Servicio Astra de su empresa. Verá este nombre en la interfaz de usuario de Astra Control Service. Tenga en cuenta que puede crear cuentas adicionales (hasta 5), si es necesario.
   - En el campo **Dirección de correo electrónico empresarial**, si tienes una cuenta de NetApp BlueXP, ingresa el correo electrónico que usas para esa cuenta aquí. Si aún no tienes una cuenta de NetApp BlueXP, utiliza la dirección de correo electrónico que introdujiste aquí cuando te registres en BlueXP.
4. Seleccione **Crear cuenta**.

Regístrese en BlueXP

El servicio Astra Control está integrado con el servicio de autenticación de NetApp BlueXP. Puedes iniciar sesión en NetApp BlueXP con tus credenciales del sitio de soporte de BlueXP o de NetApp. Si aún no tienes una cuenta del sitio de soporte de NetApp o BlueXP de NetApp, regístrate en BlueXP para poder acceder a Astra Control Service y a otros servicios cloud de NetApp. Si ya tienes una cuenta del sitio de soporte de BlueXP o NetApp y has completado el registro, podrás acceder a ella "Servicio de control Astra" Usando directamente tus credenciales del sitio de soporte de BlueXP o de NetApp.

También puedes utilizar el inicio de sesión único para iniciar sesión en BlueXP mediante las credenciales de tu directorio corporativo (identidad federada). Para obtener más información, visite la "Centro de ayuda" Y, a continuación, seleccione **Opciones de inicio de sesión de Cloud Central**.

Pasos

1. Vaya a. "BlueXP de NetApp".
2. En la parte superior derecha, selecciona **Comenzar**.
3. Seleccione **Registrarse**.
4. Rellene el formulario.

   Asegúrese de que el número de teléfono y la dirección de correo electrónico que introduce aquí son los mismos que utilizó en el formulario de registro de Astra Control anterior.

5. Seleccione **Registrarse**.

   La dirección de correo electrónico que introduzcas en estos formularios corresponde a tu ID de usuario de NetApp BlueXP. Usa este ID de usuario de BlueXP cuando te registres para obtener una nueva cuenta de Astra Control o cuando un administrador de Astra Control te invite a una cuenta existente de Astra Control.

6. Espera un correo electrónico de BlueXP de NetApp. El correo electrónico viene de la dirección saas.support@netapp.com, y puede tardar varios minutos en llegar. Asegúrese de comprobar su carpeta de spam.
7. Cuando llegue el correo electrónico, seleccione el vínculo del correo electrónico para comprobar su dirección de correo electrónico.

Resultado

Ahora tienes un inicio de sesión activo de usuario de BlueXP.

Ahora que estás registrado, puedes acceder a Astra Control directamente con tus credenciales de BlueXP desde https://astra.netapp.io.

Añada un clúster a Astra Control Service

Una vez configurado su entorno, estará listo para crear un clúster de Kubernetes y, a continuación, añadirlo al servicio Astra Control. Esto te permite utilizar el servicio Astra Control para proteger tus aplicaciones en el clúster.

Según el tipo de clúster que deba añadir a Astra Control Service, deberá realizar distintos pasos para añadir el clúster.

- "Añade un clúster público gestionado por proveedores a Astra Control Service": Utilice estos pasos para agregar un clúster que tenga una dirección IP pública y esté gestionado por un proveedor de cloud. Necesitará la cuenta principal de servicio, la cuenta de servicio o la cuenta de usuario del proveedor de cloud.
- "Añada un clúster privado gestionado por un proveedor a Astra Control Service": Utilice estos pasos para agregar un clúster que tenga una dirección IP privada y esté gestionado por un proveedor de cloud. Necesitará la cuenta principal de servicio, la cuenta de servicio o la cuenta de usuario del proveedor de cloud.

- "Añade un clúster público autogestionado a Astra Control Service": Utilice estos pasos para agregar un cluster que tenga una dirección IP pública y que sea administrado por su organización. Deberá crear un archivo kubeconfig para el cluster que desea agregar.
- "Añade un clúster privado autogestionado a Astra Control Service": Utilice estos pasos para agregar un cluster que tenga una dirección IP privada y que sea administrado por su organización. Deberá crear un archivo kubeconfig para el cluster que desea agregar.

Instala Astra Connector para gestionar los clústeres

Astra Connector es el software que reside en sus clústeres gestionados y facilita la comunicación entre el clúster gestionado y Astra Control. En el caso de los clústeres que se gestionen mediante Astra Control Service, hay dos versiones disponibles de Astra Connector:

- **Versión anterior de Astra Connector**: "Instala la versión anterior de Astra Connector" En el clúster, si tiene pensado gestionar el clúster con flujos de trabajo no nativos de Kubernetes.
- [Vista previa técnica] **Conector Astra de Kubernetes declarativo**: "Instala Astra Connector para clústeres gestionados con flujos de trabajo de Kubernetes declarativos" En el clúster si tiene pensado gestionar el clúster mediante flujos de trabajo de Kubernetes declarativos. Después de instalar Astra Connector en tu clúster, el clúster se añade automáticamente a Astra Control.

> El Astra Connector declarativo de Kubernetes solo está disponible como parte del programa para la primera adopción de Astra Control (EAP). Póngase en contacto con su representante de ventas de NetApp para obtener información sobre cómo unirse al EAP.

Instala la versión anterior de Astra Connector

Astra Control Service utiliza la versión anterior de Astra Connector para permitir la comunicación entre Astra Control Service y clústeres privados que no son nativos de Kubernetes. Tienes que instalar Astra Connector en clústeres privados que quieras gestionar con flujos de trabajo que no sean nativos de Kubernetes.

La versión anterior de Astra Connector admite los siguientes tipos de clústeres privados gestionados con flujos de trabajo no nativos de Kubernetes:

- Amazon Elastic Kubernetes Service (EKS)
- Azure Kubernetes Service (AKS)
- Google Kubernetes Engine (GKE)
- Red Hat OpenShift Service en AWS (ROSA)
- ROSA con AWS PrivateLink
- Red Hat OpenShift Container Platform en las instalaciones

Acerca de esta tarea

- Cuando realice estos pasos, ejecute estos comandos en el clúster privado que desee administrar con Astra Control Service.
- Si utiliza un host de Bastion, emita estos comandos desde la línea de comandos del host de Bastion.

Antes de empezar

- Necesita acceso al clúster privado que desea gestionar con Astra Control Service.
- Necesitas permisos de administrador de Kubernetes para instalar el operador Astra Connector en el clúster.

Pasos

1. Instale el operador Astra Connector anterior en el clúster privado que desea gestionar con flujos de trabajo que no sean nativos de Kubernetes. Cuando se ejecuta este comando, el espacio de nombres `astra-connector-operator` se crea y la configuración se aplica al espacio de nombres:

```
kubectl apply -f https://github.com/NetApp/astra-connector-operator/releases/download/23.07.0-202310251519/astraconnector_operator.yaml
```

2. Compruebe que el operador está instalado y listo:

```
kubectl get all -n astra-connector-operator
```

3. Obtén un token de API de Astra Control. Consulte la "Documentación de Astra Automation" si desea obtener instrucciones.
4. Cree el espacio de nombres de Astra-Connector:

```
kubectl create ns astra-connector
```

5. Cree el archivo Astra Connector CR y asígnele el nombre `astra-connector-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tu entorno de Astra Control y la configuración del clúster:
   - **<ASTRA_CONTROL_SERVICE_URL>**: La URL de la interfaz de usuario web del servicio de control de Astra. Por ejemplo:

     ```
     https://astra.netapp.io
     ```

   - **<ASTRA_CONTROL_SERVICE_API_TOKEN>**: El token de la API Astra Control que obtuviste en el paso anterior.
   - **<PRIVATE_AKS_CLUSTER_NAME>**: (Solo clústeres de AKS): El nombre del clúster privado del servicio de Azure Kubernetes. Elimine el comentario y rellene esta línea sólo si está agregando un cluster AKS privado.
   - **<ASTRA_CONTROL_ACCOUNT_ID>**: Obtenido de la interfaz de usuario web de Astra Control. Selecciona el icono de la figura en la parte superior derecha de la página y selecciona **Acceso API**.

```yaml
apiVersion: netapp.astraconnector.com/v1
kind: AstraConnector
metadata:
  name: astra-connector
  namespace: astra-connector
spec:
  natssync-client:
    cloud-bridge-url: <ASTRA_CONTROL_SERVICE_URL>
  imageRegistry:
    name: theotw
    secret: ""
  astra:
    token: <ASTRA_CONTROL_SERVICE_API_TOKEN>
    #clusterName: <PRIVATE_AKS_CLUSTER_NAME>
    accountId: <ASTRA_CONTROL_ACCOUNT_ID>
    acceptEULA: yes
```

6. Después de rellenar el `astra-connector-cr.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -f astra-connector-cr.yaml
```

7. Compruebe que Astra Connector está completamente implementado:

```
kubectl get all -n astra-connector
```

8. Compruebe que el clúster esté registrado en Astra Control:

```
kubectl get astraconnector -n astra-connector
```

Debería ver una salida similar a la siguiente:

```
NAME               REGISTERED   ASTRACONNECTORID
STATUS
astra-connector    true         be475ae5-1511-4eaa-9b9e-712f09b0d065
Registered with Astra
```

Toma nota del ASTRACONNECTORID, lo necesitarás cuando añadas el clúster a Astra Control.

El futuro

Ahora que ha instalado Astra Connector, está listo para añadir su clúster privado a Astra Control Service.

- "Añada un clúster privado gestionado por un proveedor a Astra Control Service": Utilice estos pasos para agregar un clúster que tenga una dirección IP privada y esté gestionado por un proveedor de cloud. Necesitará la cuenta principal de servicio, la cuenta de servicio o la cuenta de usuario del proveedor de cloud.
- "Añade un clúster privado autogestionado a Astra Control Service": Utilice estos pasos para agregar un cluster que tenga una dirección IP privada y que sea administrado por su organización. Deberá crear un archivo kubeconfig para el cluster que desea agregar.

Si quiere más información

- "Añadir un clúster"

(Vista previa técnica) Instale el Astra Connector declarativo de Kubernetes

Los clústeres gestionados mediante flujos de trabajo de Kubernetes declarativos utilizan Astra Connector para permitir la comunicación entre el clúster gestionado y Astra Control. Tienes que instalar Astra Connector en todos los clústeres que gestionarás con flujos de trabajo de Kubernetes declarativos.

Instalas el conector Astra de Kubernetes declarativo mediante comandos de Kubernetes y archivos de recursos personalizados (CR).

Acerca de esta tarea

- Cuando realice estos pasos, ejecute estos comandos en el clúster que desee gestionar con Astra Control.
- Si utiliza un host de Bastion, emita estos comandos desde la línea de comandos del host de Bastion.

Antes de empezar

- Necesitas acceder al clúster que quieras gestionar con Astra Control.
- Necesitas permisos de administrador de Kubernetes para instalar el operador Astra Connector en el clúster.

> Si el clúster está configurado con la aplicación de admisión de seguridad de POD, que es el valor predeterminado para los clústeres de Kubernetes 1,25 y posteriores, tiene que habilitar las restricciones PSA en los espacios de nombres correspondientes. Consulte "Prepare su entorno para la gestión de clústeres con Astra Control" si desea obtener instrucciones.

Pasos

1. Instale el operador Astra Connector en el clúster que desee gestionar con flujos de trabajo de Kubernetes declarativos. Cuando se ejecuta este comando, el espacio de nombres `astra-connector-operator` se crea y la configuración se aplica al espacio de nombres:

```
kubectl apply -f https://github.com/NetApp/astra-connector-
operator/releases/download/24.02.0-
202403151353/astraconnector_operator.yaml
```

2. Compruebe que el operador está instalado y listo:

```
kubectl get all -n astra-connector-operator
```

3. Obtén un token de API de Astra Control. Consulte la "Documentación de Astra Automation" si desea obtener instrucciones.
4. Cree un secreto con el token. Reemplaza <API_TOKEN> por el token que has recibido de Astra Control:

```
kubectl create secret generic astra-token \
--from-literal=apiToken=<API_TOKEN> \
-n astra-connector
```

5. Crea un secreto de Docker para extraer la imagen de Astra Connector. Sustituya los valores entre paréntesis <> por información de su entorno:

> Puedes encontrar la instancia de <ASTRA_CONTROL_ACCOUNT_ID> en la interfaz de usuario web de Astra Control. En la interfaz de usuario web, seleccione el icono de figura en la parte superior derecha de la página y seleccione **Acceso API**.

```
kubectl create secret docker-registry regcred \
--docker-username=<ASTRA_CONTROL_ACCOUNT_ID> \
--docker-password=<API_TOKEN> \
-n astra-connector \
--docker-server=cr.astra.netapp.io
```

6. Cree el archivo Astra Connector CR y asígnele el nombre `astra-connector-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tu entorno de Astra Control y la configuración del clúster:
   - <ASTRA_CONTROL_ACCOUNT_ID>: Obtenida de la interfaz de usuario web de Astra Control durante el paso anterior.
   - <CLUSTER_NAME>: El nombre que se debe asignar este clúster en Astra Control.
   - <ASTRA_CONTROL_URL>: La URL de interfaz de usuario web de Astra Control. Por ejemplo:

     ```
     https://astra.control.url
     ```

```yaml
apiVersion: astra.netapp.io/v1
kind: AstraConnector
metadata:
  name: astra-connector
  namespace: astra-connector
spec:
  astra:
    accountId: <ASTRA_CONTROL_ACCOUNT_ID>
    clusterName: <CLUSTER_NAME>
    #Only set `skipTLSValidation` to `true` when using the default
self-signed
    #certificate in a proof-of-concept environment.
    skipTLSValidation: false #Should be set to false in production
environments
    tokenRef: astra-token
  natsSyncClient:
    cloudBridgeURL: <ASTRA_CONTROL_HOST_URL>
  imageRegistry:
    name: cr.astra.netapp.io
    secret: regcred
```

7. Después de rellenar el `astra-connector-cr.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -n astra-connector -f astra-connector-cr.yaml
```

8. Compruebe que Astra Connector está completamente implementado:

```
kubectl get all -n astra-connector
```

9. Compruebe que el clúster esté registrado en Astra Control:

```
kubectl get astraconnectors.astra.netapp.io -A
```

Debería ver una salida similar a la siguiente:

```
NAMESPACE          NAME               REGISTERED   ASTRACONNECTORID
STATUS
astra-connector    astra-connector    true         00ac8-2cef-41ac-8777-
ed0583e   Registered with Astra
```

10. Compruebe que el clúster aparezca en la lista de clústeres gestionados de la página **Clusters** de la interfaz de usuario web de Astra Control.

Agregue un clúster gestionado por el proveedor

Añade un clúster público gestionado por proveedores a Astra Control Service

Después de configurar tu entorno de cloud, estarás listo para crear un clúster de Kubernetes y luego añadirlo a Astra Control Service.

- Cree un clúster de Kubernetes
- Añada el clúster a Astra Control Service
- Cambie la clase de almacenamiento predeterminada

Cree un clúster de Kubernetes

Si todavía no tiene un clúster, puede crear uno que cumpla "Requisitos del servicio Astra Control para Amazon Elastic Kubernetes Service (EKS)". Si todavía no tiene un clúster, puede crear uno que cumpla "Requisitos del servicio Astra Control para Google Kubernetes Engine (GKE)". Si todavía no tiene un clúster, puede crear uno que cumpla "Requisitos del servicio Astra Control para Azure Kubernetes Service (AKS) con Azure NetApp Files" o. "Requisitos del servicio Astra Control Service para Azure Kubernetes Service (AKS) con discos gestionados de Azure".

> Astra Control Service es compatible con clústeres AKS que utilizan Azure Active Directory (Azure AD) para la autenticación y la gestión de identidades. Cuando cree el clúster, siga las instrucciones que se indican en "documentación oficial" Para configurar el clúster de modo que use Azure AD. Debe asegurarse de que sus clústeres cumplen los requisitos de la integración de Azure AD gestionada por AKS.

Añada el clúster a Astra Control Service

Después de iniciar sesión en Astra Control Service, el primer paso es empezar a gestionar los clústeres. Antes de añadir un clúster al servicio Astra Control Service, tendrá que realizar tareas específicas y asegurarse de que el clúster cumple determinados requisitos.

Al gestionar clústeres de Azure Kubernetes Service y Google Kubernetes Engine, tenga en cuenta que tiene dos opciones para la instalación del aprovisionador de Astra Control y la gestión del ciclo de vida:

- Puedes utilizar el servicio Astra Control para gestionar automáticamente el ciclo de vida del aprovisionador Astra Control. Para hacerlo, asegúrese de que Astra Trident no esté instalado y que Astra Control Provisioner no esté habilitado en el clúster que desee gestionar con Astra Control Service. En este caso, Astra Control Service habilita automáticamente Astra Control Provisioning cuando se comienza a gestionar el clúster, y las actualizaciones del aprovisionador de Astra Control se realizan automáticamente.
- Puede gestionar el ciclo de vida de Astra Control Provisionador tú mismo. Para ello, habilite el aprovisionador de Astra Control en el clúster antes de gestionar el clúster con Astra Control Service. En este caso, Astra Control Service detecta que Astra Control Provisioning ya está habilitado y no lo reinstala ni gestiona las actualizaciones del aprovisionador de Astra Control. Consulte "Habilita el aprovisionador de Astra Control" Para seguir los pasos, habilita el aprovisionador de Astra Control.

Al gestionar clústeres de Amazon Web Services con Astra Control Service, si necesita back-ends de almacenamiento que solo puede utilizarse con el aprovisionador de Astra Control, tendrá que habilitar el aprovisionador de Astra Control manualmente en el clúster antes de gestionarlo con el servicio de Astra Control. Consulte "Habilita el aprovisionador de Astra Control" Para conocer los pasos que hay que seguir para habilitar el aprovisionador de Astra Control.

Antes de empezar

Amazon Web Services

- Debe tener el archivo JSON que contenga las credenciales del usuario de IAM que creó el clúster. "Aprenda a crear un usuario de IAM".
- Se requiere el aprovisionador de Astra Control para Amazon FSx para NetApp ONTAP. Si tienes pensado usar Amazon FSx para NetApp ONTAP como back-end de almacenamiento para tu clúster de EKS, consulte la información del aprovisionador de control de Astra en la "Requisitos del clúster de EKS".
- (Opcional) Si necesita proporcionarlo `kubectl` Consulte las instrucciones de la sección para obtener acceso al comando de un clúster a otros usuarios de IAM que no son el creador del clúster "¿Cómo puedo proporcionar acceso a otros usuarios de IAM y a otras funciones tras la creación del clúster en Amazon EKS?".
- Si tiene pensado utilizar Cloud Volumes ONTAP de NetApp como back-end de almacenamiento, debe configurar Cloud Volumes ONTAP para que funcione con Amazon Web Services. Consulte el Cloud Volumes ONTAP "documentación de configuración".

Microsoft Azure

- Debe tener el archivo JSON que contenga el resultado de la CLI de Azure cuando cree el principal del servicio. "Aprenda a configurar un director de servicios".

  También necesitará su ID de suscripción de Azure si no lo ha añadido al archivo JSON.

- Si tiene pensado utilizar Cloud Volumes ONTAP de NetApp como back-end de almacenamiento, debe configurar Cloud Volumes ONTAP para que funcione con Microsoft Azure. Consulte el Cloud Volumes ONTAP "documentación de configuración".

Google Cloud

- Debe tener el archivo de clave de cuenta de servicio para una cuenta de servicio que tenga los permisos necesarios. "Aprenda a configurar una cuenta de servicio".
- Si tiene pensado utilizar Cloud Volumes ONTAP de NetApp como back-end de almacenamiento, debe configurar Cloud Volumes ONTAP para que funcione con Google Cloud. Consulte el Cloud Volumes ONTAP "documentación de configuración".

Pasos

1. (Opcional) Si añade un clúster de Amazon EKS o desea gestionar la instalación y actualizaciones de Astra Control Provisionador, habilite Astra Control Provisionador en el clúster. Consulte "Habilita el aprovisionador de Astra Control" para pasos de habilitación.
2. Abra la interfaz de usuario web de Astra Control Service en un navegador.
3. En el Panel de control, seleccione **gestionar clúster Kubernetes**.

   Siga las instrucciones para añadir el clúster.

4. **Proveedor**: Seleccione su proveedor de cloud y, a continuación, proporcione las credenciales necesarias para crear una nueva instancia de cloud, o seleccione una instancia de cloud existente para utilizar.
5. **Amazon Web Services**: Proporcione detalles sobre su cuenta de usuario de Amazon Web Services IAM cargando un archivo JSON o pegando el contenido de ese archivo JSON desde el portapapeles.

   El archivo JSON debe contener las credenciales del usuario IAM que creó el clúster.

6. **Microsoft Azure**: Proporcione detalles sobre el principal de servicio de Azure cargando un archivo JSON o pegando el contenido de ese archivo JSON desde el portapapeles.

   El archivo JSON debe contener el resultado de la CLI de Azure al crear el principal del servicio. También puede incluir su ID de suscripción para que se agregue automáticamente a Astra. De lo contrario, deberá introducir manualmente el ID después de proporcionar JSON.

7. **Google Cloud Platform**: Proporcione el archivo de clave de cuenta de servicio cargando el archivo o pegando el contenido del portapapeles.

   Astra Control Service utiliza la cuenta de servicio para descubrir los clústeres que se ejecutan en Google Kubernetes Engine.

8. **Otros**: Esta pestaña es para uso solo con clusters autogestionados.
   a. **Nombre de la instancia de nube**: Proporcione un nombre para la nueva instancia de nube que se creará al agregar este clúster. Más información acerca de "instancias de cloud".
   b. Seleccione **Siguiente**.

      Astra Control Service muestra una lista de clústeres entre los que puede elegir.

   c. **Clúster**: Selecciona un clúster de la lista para añadirlo a Astra Control Service.

      > Al seleccionar de la lista de clusters, preste atención a la columna **Eligiblity**. Si un clúster es «no elegible» o «parcialmente elegible», pase el cursor por encima del estado para determinar si hay un problema con el clúster. Por ejemplo, podría identificar que el clúster no tiene un nodo de trabajo.

   d. Seleccione **Siguiente**.
   e. (Opcional) **Almacenamiento**: Opcionalmente, seleccione la clase de almacenamiento que desea que las aplicaciones de Kubernetes implementadas en este clúster utilicen de forma predeterminada.
9. Para seleccionar una nueva clase de almacenamiento predeterminada para el clúster, active la casilla de verificación **Asignar una nueva clase de almacenamiento predeterminada**.
10. Seleccione una nueva clase de almacenamiento predeterminada de la lista.

Cada servicio de almacenamiento de proveedor de cloud muestra la siguiente información sobre el precio, el rendimiento y la resiliencia:

- Cloud Volumes Service para Google Cloud: Información de precio, rendimiento y resiliencia
- Google Persistent Disk: No hay información de precio, rendimiento ni resiliencia disponible
- Azure NetApp Files: Información sobre rendimiento y resiliencia
- Discos administrados de Azure: No hay información de precios, rendimiento ni resiliencia disponible
- Amazon Elastic Block Store: No dispone de información de precio, rendimiento o resiliencia
- Amazon FSX para ONTAP de NetApp: Sin información de precio, rendimiento ni resiliencia disponible
- Cloud Volumes ONTAP de NetApp: No hay información de precio, rendimiento ni resiliencia disponible

Cada clase de almacenamiento puede utilizar uno de los siguientes servicios:

- "Cloud Volumes Service para Google Cloud"
- "Disco persistente de Google"
  - "Azure NetApp Files"
  - "Discos gestionados de Azure"
  - "Amazon Elastic Block Store"
  - "Amazon FSX para ONTAP de NetApp"
  - "Cloud Volumes ONTAP de NetApp"

  Más información acerca de "Clases de almacenamiento para clústeres de Amazon Web Services". Más información acerca de "Clases de almacenamiento para clústeres de AKS". Más información acerca de "Clases de almacenamiento para clústeres GKE".

  a. Seleccione **Siguiente**.
  b. **Revisar y aprobar**: Revise los detalles de la configuración.
  c. Selecciona **Add** para agregar el clúster a Astra Control Service.

Resultado

Si este es el primer clúster que se ha añadido para este proveedor de cloud, Astra Control Service crea un almacén de objetos para el proveedor de cloud para realizar backups de las aplicaciones que se ejecutan en clústeres aptos. (Cuando añada clústeres posteriores para este proveedor de cloud, no se crearán más almacenes de objetos). Si ha especificado una clase de almacenamiento predeterminada, Astra Control Service establece la clase de almacenamiento predeterminada que ha especificado. En el caso de clústeres gestionados en Amazon Web Services o Google Cloud Platform, Astra Control Service también crea una cuenta de administrador en el clúster. Estas acciones pueden tardar varios minutos.

Cambie la clase de almacenamiento predeterminada

Es posible cambiar la clase de almacenamiento predeterminada para un clúster de.

Cambie la clase de almacenamiento predeterminada con Astra Control

Puede cambiar la clase de almacenamiento predeterminada para un clúster de Astra Control. Si su clúster utiliza un servicio de fondo de almacenamiento previamente instalado, es posible que no pueda utilizar este método para cambiar la clase de almacenamiento predeterminada (la acción **establecer como predeterminada** no se puede seleccionar). En este caso, usted puede Cambie la clase de almacenamiento predeterminada con la línea de comandos.

Pasos

1. En la interfaz de usuario de Astra Control Service, seleccione **Clusters**.
2. En la página **Clusters**, seleccione el clúster que desea cambiar.
3. Seleccione la ficha **almacenamiento**.
4. Seleccione la categoría **clases de almacenamiento**.
5. Seleccione el menú **acciones** para la clase de almacenamiento que desea establecer como predeterminada.
6. Seleccione **establecer como predeterminado**.

Cambie la clase de almacenamiento predeterminada con la línea de comandos

Es posible cambiar la clase de almacenamiento predeterminada para un clúster mediante comandos de Kubernetes. Este método funciona independientemente de la configuración del clúster.

Pasos

1. Inicie sesión en su clúster de Kubernetes.
2. Enumere las clases de almacenamiento del clúster:

```
kubectl get storageclass
```

3. Quite la designación predeterminada de la clase de almacenamiento predeterminada. Sustituya <SC_NAME> por el nombre de la clase de almacenamiento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-
class":"false"}}}'
```

4. Seleccione una clase de almacenamiento diferente de forma predeterminada. Sustituya <SC_NAME> por el nombre de la clase de almacenamiento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confirme la nueva clase de almacenamiento predeterminada:

```
kubectl get storageclass
```

Añada un clúster privado gestionado por un proveedor a Astra Control Service

Puede utilizar Astra Control Service para gestionar clústeres privados de Google Kubernetes Engine (GKE). En estas instrucciones se asume que ya ha creado un clúster privado de AKS o OpenShift y preparado un método seguro para acceder de forma remota; para obtener más información sobre la creación y el acceso a clústeres privados de AKS o OpenShift, consulte la siguiente documentación:

- "Documentación de Azure para clústeres AKS privados"
- "Documentación de Azure para clústeres de OpenShift privados"

Puede utilizar Astra Control Service para gestionar clústeres privados de Azure Kubernetes Service (AKS) y clústeres privados de Red Hat OpenShift en AKS. En estas instrucciones se asume que ya ha creado un clúster privado de AKS o OpenShift y preparado un método seguro para acceder de forma remota; para obtener más información sobre la creación y el acceso a clústeres privados de AKS o OpenShift, consulte la siguiente documentación:

- "Documentación de Azure para clústeres AKS privados"
- "Documentación de Azure para clústeres de OpenShift privados"

Puede utilizar Astra Control Service para gestionar clústeres privados de Amazon Elastic Kubernetes Service (EKS). En estas instrucciones se asume que ya ha creado un clúster EKS privado y preparado un método seguro para acceder de forma remota; para obtener más información sobre la creación y el acceso a clústeres EKS privados, consulte la "Documentación de Amazon EKS".

Tienes que realizar las siguientes tareas para añadir tu clúster privado a Astra Control Service:

1. Instala Astra Connector
2. Configure el almacenamiento persistente
3. Añada el clúster gestionado por proveedores privados a Astra Control Service

Instala Astra Connector

Antes de agregar un clúster privado, tiene que instalar Astra Connector en el clúster para que Astra Control se pueda comunicar con él. Consulte "Instala la versión anterior de Astra Connector para clústeres privados gestionados con flujos de trabajo que no sean nativos de Kubernetes" si desea obtener instrucciones.

Configure el almacenamiento persistente

Configure el almacenamiento persistente para el clúster. Consulte la documentación para empezar para obtener más información sobre la configuración del almacenamiento persistente:

- "Configure Microsoft Azure con Azure NetApp Files"
- "Configure Microsoft Azure con discos gestionados de Azure"
- "Configure Amazon Web Services"
- "Configure Google Cloud"

Añada el clúster gestionado por proveedores privados a Astra Control Service

Ahora puede añadir el clúster privado a Astra Control Service.

Al gestionar clústeres de Azure Kubernetes Service y Google Kubernetes Engine, tenga en cuenta que tiene dos opciones para la instalación del aprovisionador de Astra Control y la gestión del ciclo de vida:

- Puedes utilizar el servicio Astra Control para gestionar automáticamente el ciclo de vida del aprovisionador Astra Control. Para hacerlo, asegúrese de que Astra Trident no esté instalado y que Astra Control Provisioner no esté habilitado en el clúster que desee gestionar con Astra Control Service. En este caso, Astra Control Service habilita automáticamente Astra Control Provisioning cuando se comienza a gestionar el clúster, y las actualizaciones del aprovisionador de Astra Control se realizan automáticamente.
- Puede gestionar el ciclo de vida de Astra Control Provisionador tú mismo. Para ello, habilite el aprovisionador de Astra Control en el clúster antes de gestionar el clúster con Astra Control Service. En este caso, Astra Control Service detecta que Astra Control Provisioning ya está habilitado y no lo reinstala ni gestiona las actualizaciones del aprovisionador de Astra Control. Consulte "Habilita el aprovisionador de Astra Control" Para seguir los pasos, habilita el aprovisionador de Astra Control.

Al gestionar clústeres de Amazon Web Services con Astra Control Service, si necesita back-ends de almacenamiento que solo puede utilizarse con el aprovisionador de Astra Control, tendrá que habilitar el aprovisionador de Astra Control manualmente en el clúster antes de gestionarlo con el servicio de Astra Control. Consulte "Habilita el aprovisionador de Astra Control" Para conocer los pasos que hay que seguir para habilitar el aprovisionador de Astra Control.

Antes de empezar

Amazon Web Services

- Debe tener el archivo JSON que contenga las credenciales del usuario de IAM que creó el clúster. "Aprenda a crear un usuario de IAM".
- Se requiere el aprovisionador de Astra Control para Amazon FSx para NetApp ONTAP. Si tienes pensado usar Amazon FSx para NetApp ONTAP como back-end de almacenamiento para tu clúster de EKS, consulte la información del aprovisionador de control de Astra en la "Requisitos del clúster de EKS".
- (Opcional) Si necesita proporcionarlo `kubectl` Consulte las instrucciones de la sección para obtener acceso al comando de un clúster a otros usuarios de IAM que no son el creador del clúster "¿Cómo puedo proporcionar acceso a otros usuarios de IAM y a otras funciones tras la creación del clúster en Amazon EKS?".
- Si tiene pensado utilizar Cloud Volumes ONTAP de NetApp como back-end de almacenamiento, debe configurar Cloud Volumes ONTAP para que funcione con Amazon Web Services. Consulte el Cloud Volumes ONTAP "documentación de configuración".

Microsoft Azure

- Debe tener el archivo JSON que contenga el resultado de la CLI de Azure cuando cree el principal del servicio. "Aprenda a configurar un director de servicios".

  También necesitará su ID de suscripción de Azure si no lo ha añadido al archivo JSON.

- Si tiene pensado utilizar Cloud Volumes ONTAP de NetApp como back-end de almacenamiento, debe configurar Cloud Volumes ONTAP para que funcione con Microsoft Azure. Consulte el Cloud Volumes ONTAP "documentación de configuración".

Google Cloud

- Debe tener el archivo de clave de cuenta de servicio para una cuenta de servicio que tenga los permisos necesarios. "Aprenda a configurar una cuenta de servicio".
- Si el clúster es privado, el "redes autorizadas" Debe permitir la dirección IP del servicio Astra Control:

  52.188.218.166/32

- Si tiene pensado utilizar Cloud Volumes ONTAP de NetApp como back-end de almacenamiento, debe configurar Cloud Volumes ONTAP para que funcione con Google Cloud. Consulte el Cloud Volumes ONTAP "documentación de configuración".

Pasos

1. (Opcional) Si añade un clúster de Amazon EKS o desea gestionar la instalación y actualizaciones de Astra Control Provisionador, habilite Astra Control Provisionador en el clúster. Consulte "Habilita el aprovisionador de Astra Control" para pasos de habilitación.
2. Abra la interfaz de usuario web de Astra Control Service en un navegador.
3. En el Panel de control, seleccione **gestionar clúster Kubernetes**.

   Siga las instrucciones para añadir el clúster.

4. **Proveedor**: Seleccione su proveedor de cloud y, a continuación, proporcione las credenciales necesarias para crear una nueva instancia de cloud, o seleccione una instancia de cloud existente para utilizar.

5. **Amazon Web Services**: Proporcione detalles sobre su cuenta de usuario de Amazon Web Services IAM cargando un archivo JSON o pegando el contenido de ese archivo JSON desde el portapapeles.

   El archivo JSON debe contener las credenciales del usuario IAM que creó el clúster.

6. **Microsoft Azure**: Proporcione detalles sobre el principal de servicio de Azure cargando un archivo JSON o pegando el contenido de ese archivo JSON desde el portapapeles.

   El archivo JSON debe contener el resultado de la CLI de Azure al crear el principal del servicio. También puede incluir su ID de suscripción para que se agregue automáticamente a Astra. De lo contrario, deberá introducir manualmente el ID después de proporcionar JSON.

7. **Google Cloud Platform**: Proporcione el archivo de clave de cuenta de servicio cargando el archivo o pegando el contenido del portapapeles.

   Astra Control Service utiliza la cuenta de servicio para descubrir los clústeres que se ejecutan en Google Kubernetes Engine.

8. **Otros**: Esta pestaña es para uso solo con clusters autogestionados.
   a. **Nombre de la instancia de nube**: Proporcione un nombre para la nueva instancia de nube que se creará al agregar este clúster. Más información acerca de "instancias de cloud".
   b. Seleccione **Siguiente**.

      Astra Control Service muestra una lista de clústeres entre los que puede elegir.

   c. **Clúster**: Selecciona un clúster de la lista para añadirlo a Astra Control Service.

      > Al seleccionar de la lista de clusters, preste atención a la columna **Eligiblity**. Si un clúster es «no elegible» o «parcialmente elegible», pase el cursor por encima del estado para determinar si hay un problema con el clúster. Por ejemplo, podría identificar que el clúster no tiene un nodo de trabajo.

9. Seleccione **Siguiente**.
10. (Opcional) **Almacenamiento**: Opcionalmente, seleccione la clase de almacenamiento que desea que las aplicaciones de Kubernetes implementadas en este clúster utilicen de forma predeterminada.
    a. Para seleccionar una nueva clase de almacenamiento predeterminada para el clúster, active la casilla de verificación **Asignar una nueva clase de almacenamiento predeterminada**.
    b. Seleccione una nueva clase de almacenamiento predeterminada de la lista.

Cada servicio de almacenamiento de proveedor de cloud muestra la siguiente información sobre el precio, el rendimiento y la resiliencia:

- Cloud Volumes Service para Google Cloud: Información de precio, rendimiento y resiliencia
- Google Persistent Disk: No hay información de precio, rendimiento ni resiliencia disponible
- Azure NetApp Files: Información sobre rendimiento y resiliencia
- Discos administrados de Azure: No hay información de precios, rendimiento ni resiliencia disponible
- Amazon Elastic Block Store: No dispone de información de precio, rendimiento o resiliencia
- Amazon FSX para ONTAP de NetApp: Sin información de precio, rendimiento ni resiliencia disponible
- Cloud Volumes ONTAP de NetApp: No hay información de precio, rendimiento ni resiliencia disponible

Cada clase de almacenamiento puede utilizar uno de los siguientes servicios:

- "Cloud Volumes Service para Google Cloud"
- "Disco persistente de Google"
- "Azure NetApp Files"
- "Discos gestionados de Azure"
- "Amazon Elastic Block Store"
- "Amazon FSX para ONTAP de NetApp"
- "Cloud Volumes ONTAP de NetApp"

  Más información acerca de "Clases de almacenamiento para clústeres de Amazon Web Services". Más información acerca de "Clases de almacenamiento para clústeres de AKS". Más información acerca de "Clases de almacenamiento para clústeres GKE".

c. Seleccione **Siguiente**.

d. **Revisar y aprobar**: Revise los detalles de la configuración.

e. Selecciona **Add** para agregar el clúster a Astra Control Service.

Resultado

Si este es el primer clúster que se ha añadido para este proveedor de cloud, Astra Control Service crea un almacén de objetos para el proveedor de cloud para realizar backups de las aplicaciones que se ejecutan en clústeres aptos. (Cuando añada clústeres posteriores para este proveedor de cloud, no se crearán más almacenes de objetos). Si ha especificado una clase de almacenamiento predeterminada, Astra Control Service establece la clase de almacenamiento predeterminada que ha especificado. En el caso de clústeres gestionados en Amazon Web Services o Google Cloud Platform, Astra Control Service también crea una cuenta de administrador en el clúster. Estas acciones pueden tardar varios minutos.

Cambie la clase de almacenamiento predeterminada

Es posible cambiar la clase de almacenamiento predeterminada para un clúster de.

Cambie la clase de almacenamiento predeterminada con Astra Control

Puede cambiar la clase de almacenamiento predeterminada para un clúster de Astra Control. Si su clúster utiliza un servicio de fondo de almacenamiento previamente instalado, es posible que no pueda utilizar este método para cambiar la clase de almacenamiento predeterminada (la acción **establecer como predeterminada** no se puede seleccionar). En este caso, usted puede Cambie la clase de almacenamiento predeterminada con la línea de comandos.

Pasos

1. En la interfaz de usuario de Astra Control Service, seleccione **Clusters**.
2. En la página **Clusters**, seleccione el clúster que desea cambiar.
3. Seleccione la ficha **almacenamiento**.
4. Seleccione la categoría **clases de almacenamiento**.
5. Seleccione el menú **acciones** para la clase de almacenamiento que desea establecer como predeterminada.
6. Seleccione **establecer como predeterminado**.

Cambie la clase de almacenamiento predeterminada con la línea de comandos

Es posible cambiar la clase de almacenamiento predeterminada para un clúster mediante comandos de Kubernetes. Este método funciona independientemente de la configuración del clúster.

Pasos

1. Inicie sesión en su clúster de Kubernetes.
2. Enumere las clases de almacenamiento del clúster:

```
kubectl get storageclass
```

3. Quite la designación predeterminada de la clase de almacenamiento predeterminada. Sustituya <SC_NAME> por el nombre de la clase de almacenamiento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-
class":"false"}}}'
```

4. Seleccione una clase de almacenamiento diferente de forma predeterminada. Sustituya <SC_NAME> por el nombre de la clase de almacenamiento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confirme la nueva clase de almacenamiento predeterminada:

```
kubectl get storageclass
```

Agregue un clúster autogestionado

Añade un clúster público autogestionado a Astra Control Service

Una vez configurado su entorno, estará listo para crear un clúster de Kubernetes y, a continuación, añadirlo al servicio Astra Control.

Un clúster autogestionado es un clúster que usted aprovisiona y gestiona directamente. Astra Control Service admite clústeres autogestionados que se ejecutan en un entorno de cloud público. Puede agregar un clúster autogestionado a Astra Control Service cargando un `kubeconfig.yaml` archivo. Deberá asegurarse de que el clúster cumple los requisitos que se indican aquí.

Distribuciones de Kubernetes compatibles

Puede utilizar Astra Control Service para gestionar los siguientes tipos de clústeres públicos autogestionados:

Distribución de Kubernetes	Versiones compatibles
Kubernetes (ascendente)	1,27 a 1,29
Motor Kubernetes de rancher (RKE)	RKE 1: Versiones 1.24.17, 1.25.13, 1.26.8 con Rancher Manager 2.7.9 RKE 2: Versiones 1.23.16 y 1.24.13 con Rancher Manager 2.6.13 RKE 2: Versiones 1.24.17, 1.25.14, 1.26.9 con Rancher Manager 2.7.9
OpenShift Container Platform de Red Hat	4,12 hasta 4,14

En estas instrucciones se asume que ya ha creado un clúster autogestionado.

- Añada el clúster a Astra Control Service
- Cambie la clase de almacenamiento predeterminada

Añada el clúster a Astra Control Service

Después de iniciar sesión en Astra Control Service, el primer paso es empezar a gestionar los clústeres. Antes de añadir un clúster al servicio Astra Control Service, tendrá que realizar tareas específicas y asegurarse de que el clúster cumple determinados requisitos.

Antes de empezar

Un clúster autogestionado es un clúster que usted aprovisiona y gestiona directamente. Astra Control Service admite clústeres autogestionados que se ejecutan en un entorno de cloud público. Los clústeres autogestionados pueden utilizar Astra Control Provisioner para interactuar con los servicios de almacenamiento de NetApp o pueden usar controladores de la interfaz de almacenamiento de contenedores (CSI) para interactuar con Amazon Elastic Block Store (EBS), los discos gestionados de Azure y el disco persistente de Google.

Astra Control Service es compatible con clústeres autogestionados que utilizan las siguientes distribuciones de Kubernetes:

- OpenShift Container Platform de Red Hat
- Motor Kubernetes del rancher
- Subida de Kubernetes

Su clúster autogestionado debe cumplir con los siguientes requisitos:

- El clúster debe estar accesible a través de Internet.
- Si está utilizando o planea utilizar almacenamiento habilitado con controladores CSI, se deben instalar los controladores CSI adecuados en el clúster. Para obtener más información sobre el uso de los controladores CSI para integrar el almacenamiento, consulte la documentación del servicio de almacenamiento.
- Tiene acceso al archivo kubeconfig de cluster que incluye solo un elemento de contexto. Siga "estas instrucciones" para generar un archivo kubeconfig.
- Si va a agregar el clúster mediante un archivo kubeconfig que hace referencia a una entidad de certificación (CA) privada, agregue la siguiente línea al `cluster` sección del archivo kubeconfig. Esto permite a Astra Control añadir el clúster:

  ```
  insecure-skip-tls-verify: true
  ```

- **Sólo rancher**: Al administrar clústeres de aplicaciones en un entorno Rancher, modifique el contexto predeterminado del clúster de aplicaciones en el archivo kubeconfig proporcionado por Rancher para utilizar un contexto de plano de control en lugar del contexto del servidor API Rancher. Esto reduce la carga en el servidor API de Rancher y mejora el rendimiento.
- **Requisitos del aprovisionador de Astra Control**: Debes tener un aprovisionador de Astra Control configurado correctamente, incluidos sus componentes de Astra Trident, para gestionar clústeres.
  - **Revise los requisitos del entorno de Astra Trident**: Antes de instalar o actualizar el aprovisionador de Astra Control, revise el "compatibles con front-ends, back-ends y configuraciones de host".
  - **Habilitar la funcionalidad de aprovisionamiento de Astra Control**: Se recomienda instalar Astra Trident 23,10 o posterior y activar "Funcionalidad de almacenamiento avanzada de Astra Control Provisioning". En las siguientes versiones, Astra Control no será compatible con Astra Trident si el aprovisionador de Astra Control también no está habilitado.
  - **Configurar un backend de almacenamiento**: Al menos un backend de almacenamiento debe ser "Configuradas en Astra Trident" en el clúster.
  - **Configure una clase de almacenamiento**: Al menos una clase de almacenamiento debe ser "Configuradas en Astra Trident" en el clúster. Si se configura una clase de almacenamiento

predeterminada, asegúrese de que es la clase de almacenamiento **Only** que tiene la anotación predeterminada.

- **Configure un controlador de instantáneas de volumen e instale una clase de instantáneas de volumen**: "Instale una controladora Snapshot de volumen" Para poder crear instantáneas en Astra Control. "Cree" al menos uno `VolumeSnapshotClass` Mediante Astra Trident.

Pasos

1. En el Panel de control, seleccione **gestionar clúster Kubernetes**.

   Siga las instrucciones para añadir el clúster.

2. **Proveedor**: Selecciona la pestaña **Otro** para agregar detalles sobre tu cluster autogestionado.
   a. **Otros**: Proporcione detalles sobre su cluster autogestionado cargando un `kubeconfig.yaml` o bien, pegue el contenido de `kubeconfig.yaml` desde el portapapeles.

   > Si crea el suyo propio `kubeconfig` file, debe definir sólo un elemento de contexto **uno** en él. Consulte "Documentación de Kubernetes" para obtener información acerca de cómo crear `kubeconfig` archivos.

3. **Nombre de credencial**: Proporciona un nombre para la credencial de clúster autogestionada que estás cargando en Astra Control. De forma predeterminada, el nombre de las credenciales se completa automáticamente como nombre del clúster.
4. **Identificador de ruta privado**: Este campo es solo para uso con clusters privados.
5. Seleccione **Siguiente**.
6. (Opcional) **Almacenamiento**: Opcionalmente, seleccione la clase de almacenamiento que desea que las aplicaciones de Kubernetes implementadas en este clúster utilicen de forma predeterminada.
   a. Para seleccionar una nueva clase de almacenamiento predeterminada para el clúster, active la casilla de verificación **Asignar una nueva clase de almacenamiento predeterminada**.
   b. Seleccione una nueva clase de almacenamiento predeterminada de la lista.

   > Cada servicio de almacenamiento de proveedor de cloud muestra la siguiente información sobre el precio, el rendimiento y la resiliencia:
   >
   > - Cloud Volumes Service para Google Cloud: Información de precio, rendimiento y resiliencia
   > - Google Persistent Disk: No hay información de precio, rendimiento ni resiliencia disponible
   > - Azure NetApp Files: Información sobre rendimiento y resiliencia
   > - Discos administrados de Azure: No hay información de precios, rendimiento ni resiliencia disponible
   > - Amazon Elastic Block Store: No dispone de información de precio, rendimiento o resiliencia
   > - Amazon FSX para ONTAP de NetApp: Sin información de precio, rendimiento ni resiliencia disponible
   > - Cloud Volumes ONTAP de NetApp: No hay información de precio, rendimiento ni resiliencia disponible

Cada clase de almacenamiento puede utilizar uno de los siguientes servicios:

- "Cloud Volumes Service para Google Cloud"
- "Disco persistente de Google"
  - "Azure NetApp Files"
  - "Discos gestionados de Azure"
  - "Amazon Elastic Block Store"
  - "Amazon FSX para ONTAP de NetApp"
  - "Cloud Volumes ONTAP de NetApp"

    Más información acerca de "Clases de almacenamiento para clústeres de Amazon Web Services". Más información acerca de "Clases de almacenamiento para clústeres de AKS". Más información acerca de "Clases de almacenamiento para clústeres GKE".

c. Seleccione **Siguiente**.

d. **Revisar y aprobar**: Revise los detalles de la configuración.

e. Selecciona **Add** para agregar el clúster a Astra Control Service.

Cambie la clase de almacenamiento predeterminada

Es posible cambiar la clase de almacenamiento predeterminada para un clúster de.

Cambie la clase de almacenamiento predeterminada con Astra Control

Puede cambiar la clase de almacenamiento predeterminada para un clúster de Astra Control. Si su clúster utiliza un servicio de fondo de almacenamiento previamente instalado, es posible que no pueda utilizar este método para cambiar la clase de almacenamiento predeterminada (la acción **establecer como predeterminada** no se puede seleccionar). En este caso, usted puede Cambie la clase de almacenamiento predeterminada con la línea de comandos.

Pasos

1. En la interfaz de usuario de Astra Control Service, seleccione **Clusters**.
2. En la página **Clusters**, seleccione el clúster que desea cambiar.
3. Seleccione la ficha **almacenamiento**.
4. Seleccione la categoría **clases de almacenamiento**.
5. Seleccione el menú **acciones** para la clase de almacenamiento que desea establecer como predeterminada.
6. Seleccione **establecer como predeterminado**.

Cambie la clase de almacenamiento predeterminada con la línea de comandos

Es posible cambiar la clase de almacenamiento predeterminada para un clúster mediante comandos de Kubernetes. Este método funciona independientemente de la configuración del clúster.

Pasos

1. Inicie sesión en su clúster de Kubernetes.
2. Enumere las clases de almacenamiento del clúster:

```
kubectl get storageclass
```

3. Quite la designación predeterminada de la clase de almacenamiento predeterminada. Sustituya <SC_NAME> por el nombre de la clase de almacenamiento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-
class":"false"}}}'
```

4. Seleccione una clase de almacenamiento diferente de forma predeterminada. Sustituya <SC_NAME> por el nombre de la clase de almacenamiento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confirme la nueva clase de almacenamiento predeterminada:

```
kubectl get storageclass
```

Añade un clúster privado autogestionado a Astra Control Service

Una vez configurado su entorno, estará listo para crear un clúster de Kubernetes y, a continuación, añadirlo al servicio Astra Control.

Un clúster autogestionado es un clúster que usted aprovisiona y gestiona directamente. Astra Control Service admite clústeres autogestionados que se ejecutan en un entorno de cloud público. Puede agregar un clúster autogestionado a Astra Control Service cargando un `kubeconfig.yaml` archivo. Deberá asegurarse de que el clúster cumple los requisitos que se indican aquí.

Distribuciones de Kubernetes compatibles

Puede utilizar Astra Control Service para gestionar los siguientes tipos de clústeres privados autogestionados:

Distribución de Kubernetes	Versiones compatibles
Kubernetes (ascendente)	1,27 a 1,29
Motor Kubernetes de rancher (RKE)	RKE 1: Versiones 1.24.17, 1.25.13, 1.26.8 con Rancher Manager 2.7.9 RKE 2: Versiones 1.23.16 y 1.24.13 con Rancher Manager 2.6.13 RKE 2: Versiones 1.24.17, 1.25.14, 1.26.9 con Rancher Manager 2.7.9
OpenShift Container Platform de Red Hat	4,12 hasta 4,14

En estas instrucciones se asume que ya ha creado un clúster privado y ha preparado un método seguro para

acceder de forma remota a él.

Tienes que realizar las siguientes tareas para añadir tu clúster privado a Astra Control Service:

1. Instala Astra Connector
2. Configure el almacenamiento persistente
3. Añada el clúster autogestionado privado a Astra Control Service

Instala Astra Connector

Antes de agregar un clúster privado, tiene que instalar Astra Connector en el clúster para que Astra Control se pueda comunicar con él. Consulte "Instala la versión anterior de Astra Connector para clústeres privados gestionados con flujos de trabajo que no sean nativos de Kubernetes" si desea obtener instrucciones.

Configure el almacenamiento persistente

Configure el almacenamiento persistente para el clúster. Consulte la documentación para empezar para obtener más información sobre la configuración del almacenamiento persistente:

- "Configure Microsoft Azure con Azure NetApp Files"
- "Configure Microsoft Azure con discos gestionados de Azure"
- "Configure Amazon Web Services"
- "Configure Google Cloud"

Añada el clúster autogestionado privado a Astra Control Service

Ahora puede añadir el clúster privado a Astra Control Service.

Antes de empezar

Un clúster autogestionado es un clúster que usted aprovisiona y gestiona directamente. Astra Control Service admite clústeres autogestionados que se ejecutan en un entorno de cloud público. Los clústeres autogestionados pueden utilizar Astra Control Provisioner para interactuar con los servicios de almacenamiento de NetApp o pueden usar controladores de la interfaz de almacenamiento de contenedores (CSI) para interactuar con Amazon Elastic Block Store (EBS), los discos gestionados de Azure y el disco persistente de Google.

Astra Control Service es compatible con clústeres autogestionados que utilizan las siguientes distribuciones de Kubernetes:

- OpenShift Container Platform de Red Hat
- Motor Kubernetes del rancher
- Subida de Kubernetes

Su clúster autogestionado debe cumplir con los siguientes requisitos:

- El clúster debe estar accesible a través de Internet.
- Si está utilizando o planea utilizar almacenamiento habilitado con controladores CSI, se deben instalar los controladores CSI adecuados en el clúster. Para obtener más información sobre el uso de los controladores CSI para integrar el almacenamiento, consulte la documentación del servicio de almacenamiento.
- Tiene acceso al archivo kubeconfig de cluster que incluye solo un elemento de contexto. Siga "estas instrucciones" para generar un archivo kubeconfig.
- Si va a agregar el clúster mediante un archivo kubeconfig que hace referencia a una entidad de certificación (CA) privada, agregue la siguiente línea al `cluster` sección del archivo kubeconfig. Esto permite a Astra Control añadir el clúster:

  ```
  insecure-skip-tls-verify: true
  ```

- **Sólo rancher**: Al administrar clústeres de aplicaciones en un entorno Rancher, modifique el contexto predeterminado del clúster de aplicaciones en el archivo kubeconfig proporcionado por Rancher para utilizar un contexto de plano de control en lugar del contexto del servidor API Rancher. Esto reduce la carga en el servidor API de Rancher y mejora el rendimiento.
- **Requisitos del aprovisionador de Astra Control**: Debes tener un aprovisionador de Astra Control configurado correctamente, incluidos sus componentes de Astra Trident, para gestionar clústeres.
  - **Revise los requisitos del entorno de Astra Trident**: Antes de instalar o actualizar el aprovisionador de Astra Control, revise el "compatibles con front-ends, back-ends y configuraciones de host".
  - **Habilitar la funcionalidad de aprovisionamiento de Astra Control**: Se recomienda instalar Astra Trident 23,10 o posterior y activar "Funcionalidad de almacenamiento avanzada de Astra Control Provisioning". En las siguientes versiones, Astra Control no será compatible con Astra Trident si el aprovisionador de Astra Control también no está habilitado.
  - **Configurar un backend de almacenamiento**: Al menos un backend de almacenamiento debe ser "Configuradas en Astra Trident" en el clúster.
  - **Configure una clase de almacenamiento**: Al menos una clase de almacenamiento debe ser "Configuradas en Astra Trident" en el clúster. Si se configura una clase de almacenamiento

predeterminada, asegúrese de que es la clase de almacenamiento **Only** que tiene la anotación predeterminada.

- **Configure un controlador de instantáneas de volumen e instale una clase de instantáneas de volumen**: "Instale una controladora Snapshot de volumen" Para poder crear instantáneas en Astra Control. "Cree" al menos uno `VolumeSnapshotClass` Mediante Astra Trident.

Pasos

1. En el Panel de control, seleccione **gestionar clúster Kubernetes**.

   Siga las instrucciones para añadir el clúster.

2. **Proveedor**: Selecciona la pestaña **Otro** para agregar detalles sobre tu cluster autogestionado.
3. **Otros**: Proporcione detalles sobre su cluster autogestionado cargando un `kubeconfig.yaml` o bien, pegue el contenido de `kubeconfig.yaml` desde el portapapeles.

   > Si crea el suyo propio `kubeconfig` file, debe definir sólo un elemento de contexto **uno** en él. Consulte "estas instrucciones" para obtener información acerca de cómo crear `kubeconfig` archivos.

4. **Nombre de credencial**: Proporciona un nombre para la credencial de clúster autogestionada que estás cargando en Astra Control. De forma predeterminada, el nombre de las credenciales se completa automáticamente como nombre del clúster.
5. **Identificador de ruta privado**: Introduce el identificador de ruta privado, que puedes obtener del Astra Connector. Si consulta el Astra Connector a través del `kubectl get astraconnector -n astra-connector` comando, el identificador de ruta privada se denomina `ASTRACONNECTORID`.

   > El identificador de ruta privada es el nombre asociado con Astra Connector que permite gestionar un clúster de Kubernetes privado con Astra. En este contexto, un clúster privado es un clúster de Kubernetes que no expone su servidor API a Internet.

6. Seleccione **Siguiente**.
7. (Opcional) **Almacenamiento**: Opcionalmente, seleccione la clase de almacenamiento que desea que las aplicaciones de Kubernetes implementadas en este clúster utilicen de forma predeterminada.
   a. Para seleccionar una nueva clase de almacenamiento predeterminada para el clúster, active la casilla de verificación **Asignar una nueva clase de almacenamiento predeterminada**.
   b. Seleccione una nueva clase de almacenamiento predeterminada de la lista.

Cada servicio de almacenamiento de proveedor de cloud muestra la siguiente información sobre el precio, el rendimiento y la resiliencia:

- Cloud Volumes Service para Google Cloud: Información de precio, rendimiento y resiliencia
- Google Persistent Disk: No hay información de precio, rendimiento ni resiliencia disponible
- Azure NetApp Files: Información sobre rendimiento y resiliencia
- Discos administrados de Azure: No hay información de precios, rendimiento ni resiliencia disponible
- Amazon Elastic Block Store: No dispone de información de precio, rendimiento o resiliencia
- Amazon FSX para ONTAP de NetApp: Sin información de precio, rendimiento ni resiliencia disponible
- Cloud Volumes ONTAP de NetApp: No hay información de precio, rendimiento ni resiliencia disponible

Cada clase de almacenamiento puede utilizar uno de los siguientes servicios:

- "Cloud Volumes Service para Google Cloud"
- "Disco persistente de Google"
- "Azure NetApp Files"
- "Discos gestionados de Azure"
- "Amazon Elastic Block Store"
- "Amazon FSX para ONTAP de NetApp"
- "Cloud Volumes ONTAP de NetApp"

  Más información acerca de "Clases de almacenamiento para clústeres de Amazon Web Services". Más información acerca de "Clases de almacenamiento para clústeres de AKS". Más información acerca de "Clases de almacenamiento para clústeres GKE".

c. Seleccione **Siguiente**.

d. **Revisar y aprobar**: Revise los detalles de la configuración.

e. Selecciona **Add** para agregar el clúster a Astra Control Service.

Cambie la clase de almacenamiento predeterminada

Es posible cambiar la clase de almacenamiento predeterminada para un clúster de.

Cambie la clase de almacenamiento predeterminada con Astra Control

Puede cambiar la clase de almacenamiento predeterminada para un clúster de Astra Control. Si su clúster utiliza un servicio de fondo de almacenamiento previamente instalado, es posible que no pueda utilizar este método para cambiar la clase de almacenamiento predeterminada (la acción **establecer como predeterminada** no se puede seleccionar). En este caso, usted puede Cambie la clase de almacenamiento predeterminada con la línea de comandos.

Pasos

1. En la interfaz de usuario de Astra Control Service, seleccione **Clusters**.
2. En la página **Clusters**, seleccione el clúster que desea cambiar.
3. Seleccione la ficha **almacenamiento**.
4. Seleccione la categoría **clases de almacenamiento**.
5. Seleccione el menú **acciones** para la clase de almacenamiento que desea establecer como predeterminada.
6. Seleccione **establecer como predeterminado**.

Cambie la clase de almacenamiento predeterminada con la línea de comandos

Es posible cambiar la clase de almacenamiento predeterminada para un clúster mediante comandos de Kubernetes. Este método funciona independientemente de la configuración del clúster.

Pasos

1. Inicie sesión en su clúster de Kubernetes.
2. Enumere las clases de almacenamiento del clúster:

```
kubectl get storageclass
```

3. Quite la designación predeterminada de la clase de almacenamiento predeterminada. Sustituya <SC_NAME> por el nombre de la clase de almacenamiento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-
class":"false"}}}'
```

4. Seleccione una clase de almacenamiento diferente de forma predeterminada. Sustituya <SC_NAME> por el nombre de la clase de almacenamiento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confirme la nueva clase de almacenamiento predeterminada:

```
kubectl get storageclass
```

Comprueba la versión de Astra Trident

Para añadir un clúster autogestionado que utilice el aprovisionador de Astra Control o Astra Trident para los servicios de almacenamiento, asegúrese de que la versión instalada de Astra Trident sea la versión 23,10 o la más reciente.

Pasos

1. Determine la versión de Astra Trident que ejecuta:

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

Si Astra Trident está instalado, verá una salida similar a la siguiente:

```
NAME      VERSION
trident   24.02.0
```

Si Astra Trident no está instalado, verá una salida similar a la siguiente:

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

2. Debe realizar una de las siguientes acciones:
   - Si utiliza Astra Trident 23,01 o una versión anterior, utilice estos "instrucciones" Para actualizar a una versión más reciente de Astra Trident antes de actualizar a Astra Control Provisioner. Puede hacerlo "realice una actualización directa" Para Astra Control Provisioner 24,02 si tu Astra Trident está en una ventana de cuatro versiones de la versión 24,02. Por ejemplo, puedes actualizar directamente de Astra Trident 23,04 a Astra Control Provisioner 24,02.
   - Si utiliza Astra Trident 23,10 o una versión posterior, compruebe que el aprovisionador de Astra Control haya sido "activado". El aprovisionador de Astra Control no funcionará con versiones de Astra Control Center anteriores a la 23,10. "Actualiza tu aprovisionador de Astra Control" De modo que tiene la misma versión que Astra Control Center que vas a actualizar para acceder a la funcionalidad más reciente.
3. Asegúrese de que los pods estén ejecutando:

```
kubectl get pods -n trident
```

4. Compruebe si las clases de almacenamiento utilizan los controladores Astra Trident compatibles. El nombre del aprovisionador debe ser `csi.trident.netapp.io`. Consulte el siguiente ejemplo:

```
kubectl get sc
```

Respuesta de ejemplo:

```
NAME                    PROVISIONER                    RECLAIMPOLICY
VOLUMEBINDINGMODE   ALLOWVOLUMEEXPANSION   AGE
ontap-gold (default)    csi.trident.netapp.io          Delete
Immediate           true                   5d23h
```

Cree un archivo kubeconfig

Puede añadir un clúster a Astra Control Service mediante un archivo kubeconfig. En función del tipo de cluster que desee agregar, es posible que necesite crear manualmente un archivo kubeconfig para el cluster mediante pasos específicos.

- Cree un archivo kubeconfig para los clústeres de Amazon EKS
- Cree un archivo kubeconfig para los clústeres de Red Hat OpenShift Service en AWS (ROSA)
- Cree un archivo kubeconfig para otros tipos de clusters

Cree un archivo kubeconfig para los clústeres de Amazon EKS

Siga estas instrucciones para crear un archivo kubeconfig y un secreto de token permanente para los clústeres de Amazon EKS. Se necesita un secreto de token permanente para los clústeres alojados en EKS.

Pasos

1. Siga las instrucciones de la documentación de Amazon para generar un archivo kubeconfig:

   "Creación o actualización de un archivo kubeconfig para un clúster de Amazon EKS"

2. Cree una cuenta de servicio del siguiente modo:

   a. Cree un archivo de cuenta de servicio llamado `astracontrol-service-account.yaml`.

      Ajuste el nombre de la cuenta de servicio según sea necesario. El espacio de nombres `kube-system` es necesario para estos pasos. Si cambia aquí el nombre de la cuenta de servicio, debe aplicar los mismos cambios en los siguientes pasos.

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

+

```yaml
apiVersion: v1
kind: ServiceAccount
metadata:
  name: astra-admin-account
  namespace: kube-system
```

3. Aplicar la cuenta de servicio:

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

4. Cree un `ClusterRoleBinding` archivo llamado `astracontrol-clusterrolebinding.yaml`.

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

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: astra-admin-binding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-admin
subjects:
- kind: ServiceAccount
  name: astra-admin-account
  namespace: kube-system
```

5. Aplique el enlace de roles del clúster:

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

6. Se ha llamado a crear un archivo secreto de token de cuenta de servicio `astracontrol-secret.yaml`.

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

```yaml
apiVersion: v1
kind: Secret
metadata:
  annotations:
    kubernetes.io/service-account.name: astra-admin-account
  name: astra-admin-account
  namespace: kube-system
type: kubernetes.io/service-account-token
```

7. Aplique el secreto de token:

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

8. Recupere el secreto de token:

```
kubectl get secret astra-admin-account -n kube-system -o
jsonpath='{.data.token}' | base64 -d
```

9. Sustituya el `user` Sección del archivo kubeconfig de AWS EKS con el token, como se muestra en el

siguiente ejemplo:

```
user:
    token: k8s-aws-
v1.aHR0cHM6Ly9zdHMudXMtd2VzdC0yLmFtYXpvbmF3cy5jb20vP0FjdGlvbj1HZXRDYWxsZ
XJJZGVudGl0eSZWZXJzaW9uPTIwMTEtMDYtMTUmWC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQ
y1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBM1JEWDdKU0haWU9LSEQ2SyUyRjIwMjMwN
DAzJTJGdXMtd2VzdC0yJTJGc3RzJTJGYXdzNF9yZXF1ZXN0JlgtQW16LURhdGU9MjAyMzA0M
DNUMjA0MzQwWiZYLUFtei1FeHBpcmVzPTYwJlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCUzQ
ngtazhzLWF3cy1pZCZYLUFtei1TaWduYXR1cmU9YjU4ZWM0NzdiM2NkZGYxNGRhNzU4MGI2Z
WQ2zY2NzI2YWIwM2UyNThjMjRhNTJjNmVhNjc4MTRlNjJkOTg2Mg
```

Cree un archivo kubeconfig para los clústeres de Red Hat OpenShift Service en AWS (ROSA)

Siga estas instrucciones para crear un archivo kubeconfig para clústeres de Red Hat OpenShift Service en AWS (ROSA).

Pasos

1. Inicie sesión en el clúster ROSA.
2. Cree una cuenta de servicio:

```
oc create sa astracontrol-service-account
```

3. Añada un rol de clúster:

```
oc adm policy add-cluster-role-to-user cluster-admin -z astracontrol-
service-account
```

4. Con el siguiente ejemplo, cree un archivo de configuración secreto de cuenta de servicio:

```
<strong>secret-astra-sa.yaml</strong>
```

```
apiVersion: v1
kind: Secret
metadata:
  name: secret-astracontrol-service-account
  annotations:
    kubernetes.io/service-account.name: "astracontrol-service-account"
type: kubernetes.io/service-account-token
```

5. Cree el secreto:

```
oc create -f secret-astra-sa.yaml
```

6. Edite la cuenta de servicio que ha creado y agregue el nombre secreto de la cuenta de servicio de Astra Control a `secrets` sección:

```
oc edit sa astracontrol-service-account
```

```
apiVersion: v1
imagePullSecrets:
- name: astracontrol-service-account-dockercfg-dvfcd
kind: ServiceAccount
metadata:
  creationTimestamp: "2023-08-04T04:18:30Z"
  name: astracontrol-service-account
  namespace: default
  resourceVersion: "169770"
  uid: 965fa151-923f-4fbd-9289-30cad15998ac
secrets:
- name: astracontrol-service-account-dockercfg-dvfcd
- name: secret-astracontrol-service-account ####ADD THIS ONLY####
```

7. Enumere los secretos de la cuenta de servicio, reemplazando `<CONTEXT>` con el contexto correcto para su instalación:

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

El final de la salida debe ser similar a lo siguiente:

```
"secrets": [
{ "name": "astracontrol-service-account-dockercfg-dvfcd"},
{ "name": "secret-astracontrol-service-account"}
]
```

Los índices de cada elemento de la `secrets` la matriz comienza con 0. En el ejemplo anterior, el índice para `astracontrol-service-account-dockercfg-dvfcd` sería 0 y el índice para `secret-astracontrol-service-account` sería 1. En la salida, anote el número de índice del secreto de la cuenta de servicio. Necesitará este número de índice en el siguiente paso.

8. Genere la kubeconfig de la siguiente manera:

   a. Cree un `create-kubeconfig.sh` archivo. Sustituya `TOKEN_INDEX` al principio de la secuencia de comandos siguiente con el valor correcto.

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

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

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

CONTEXT=$(kubectl config current-context)

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

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

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

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

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

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

# Create token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
```

```
  set-credentials ${CONTEXT}-${NAMESPACE}-token-user \
  --token ${TOKEN}

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

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

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

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

b. Origen de los comandos para aplicarlos al clúster de Kubernetes.

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

9. (Opcional) cambie el nombre de la Marca de prestigio por un nombre significativo para el clúster.

```
mv kubeconfig-sa YOUR_CLUSTER_NAME_kubeconfig
```

Cree un archivo kubeconfig para otros tipos de clusters

Siga estas instrucciones para crear un archivo kubeconfig de rol limitado o ampliado para Rancher, upstream Kubernetes y Red Hat OpenShift clusters.

Para los clústeres que se gestionan mediante kubeconfig, opcionalmente puede crear un rol de administrador de permisos limitado o de permisos ampliados para Astra Control Service.

Este procedimiento le ayuda a crear un kubeconfig independiente si cualquiera de los siguientes escenarios se aplica a su entorno:

- Deseas limitar los permisos de Astra Control a los clústeres que gestiona
- Usas varios contextos y no puedes usar el comando predeterminado de Astra Control configurado durante la instalación o un rol limitado con un solo contexto no funcionará en tu entorno

Antes de empezar

Asegúrese de que tiene lo siguiente para el clúster que tiene intención de administrar antes de completar los pasos del procedimiento:

- A. "versión compatible" de kubectl está instalado.
- Acceso kubectl al clúster que pretendes añadir y gestionar mediante Astra Control Service

> Para este procedimiento, no necesita acceso kubectl al clúster que ejecuta Astra Control Service.

- Una imagen de referencia activa para el clúster que pretende gestionar con derechos de administrador del clúster para el contexto activo

Pasos

1. Cree una cuenta de servicio:
   a. Cree un archivo de cuenta de servicio llamado `astracontrol-service-account.yaml`.

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

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

   b. Aplicar la cuenta de servicio:

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

2. Cree uno de los siguientes roles de clúster con permisos suficientes para que Astra Control gestione un clúster:

Rol de clúster limitado

Este rol contiene los permisos mínimos necesarios para que Astra Control gestione un clúster:

a. Cree un `ClusterRole` archivo llamado, por ejemplo, `astra-admin-account.yaml`.

```
<strong>astra-admin-account.yaml</strong>
```

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: astra-admin-account
rules:

# Get, List, Create, and Update all resources
# Necessary to backup and restore all resources in an app
- apiGroups:
  - '*'
  resources:
  - '*'
  verbs:
  - get
  - list
  - create
  - patch

# Delete Resources
# Necessary for in-place restore and AppMirror failover
- apiGroups:
  - ""
  - apps
  - autoscaling
  - batch
  - crd.projectcalico.org
  - extensions
  - networking.k8s.io
  - policy
  - rbac.authorization.k8s.io
  - snapshot.storage.k8s.io
  - trident.netapp.io
  resources:
  - configmaps
  - cronjobs
  - daemonsets
  - deployments
```

```
    - horizontalpodautoscalers
    - ingresses
    - jobs
    - namespaces
    - networkpolicies
    - persistentvolumeclaims
    - poddisruptionbudgets
    - pods
    - podtemplates
    - replicasets
    - replicationcontrollers
    - replicationcontrollers/scale
    - rolebindings
    - roles
    - secrets
    - serviceaccounts
    - services
    - statefulsets
    - tridentmirrorrelationships
    - tridentsnapshotinfos
    - volumesnapshots
    - volumesnapshotcontents
    verbs:
    - delete

  # Watch resources
  # Necessary to monitor progress
  - apiGroups:
    - ""
    resources:
    - pods
    - replicationcontrollers
    - replicationcontrollers/scale
    verbs:
    - watch

  # Update resources
  - apiGroups:
    - ""
    - build.openshift.io
    - image.openshift.io
    resources:
    - builds/details
    - replicationcontrollers
    - replicationcontrollers/scale
    - imagestreams/layers
```

```
  - imagestreamtags
  - imagetags
  verbs:
  - update
```

b. (Solo para clústeres de OpenShift) Añada lo siguiente al final del `astra-admin-account.yaml` archivo:

```
# OpenShift security
- apiGroups:
  - security.openshift.io
  resources:
  - securitycontextconstraints
  verbs:
  - use
  - update
```

c. Aplique el rol de clúster:

```
kubectl apply -f astra-admin-account.yaml
```

Rol del clúster ampliado

Este rol contiene permisos ampliados para que un clúster lo gestione Astra Control. Puedes usar este rol si utilizas varios contextos y no puedes utilizar el comando kubeconfig predeterminado de Astra Control configurado durante la instalación o un rol limitado con un único contexto no funcionará en tu entorno:

> Lo siguiente `ClusterRole` Los pasos son un ejemplo general de Kubernetes. Consulte la documentación de la distribución de Kubernetes para obtener instrucciones específicas de su entorno.

a. Cree un `ClusterRole` archivo llamado, por ejemplo, `astra-admin-account.yaml`.

```
<strong>astra-admin-account.yaml</strong>
```

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: astra-admin-account
rules:
- apiGroups:
  - '*'
  resources:
  - '*'
  verbs:
  - '*'
- nonResourceURLs:
  - '*'
  verbs:
  - '*'
```

b. Aplique el rol de clúster:

```
kubectl apply -f astra-admin-account.yaml
```

3. Cree el enlace de rol de clúster para el rol del clúster a la cuenta de servicio:

a. Cree un `ClusterRoleBinding` archivo llamado `astracontrol-clusterrolebinding.yaml`.

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

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

b. Aplique el enlace de roles del clúster:

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

4. Crear y aplicar el secreto de token:
   a. Cree un archivo secreto de token llamado `secret-astracontrol-service-account.yaml`.

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

```
apiVersion: v1
kind: Secret
metadata:
  name: secret-astracontrol-service-account
  namespace: default
  annotations:
    kubernetes.io/service-account.name: "astracontrol-service-
account"
type: kubernetes.io/service-account-token
```

   b. Aplique el secreto de token:

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

5. Agregue el secreto de token a la cuenta de servicio agregando su nombre a la `secrets` array (la última línea del siguiente ejemplo):

```
kubectl edit sa astracontrol-service-account
```

```
apiVersion: v1
imagePullSecrets:
- name: astracontrol-service-account-dockercfg-48xhx
kind: ServiceAccount
metadata:
  annotations:
    kubectl.kubernetes.io/last-applied-configuration: |

{"apiVersion":"v1","kind":"ServiceAccount","metadata":{"annotations":{},
"name":"astracontrol-service-account","namespace":"default"}}
  creationTimestamp: "2023-06-14T15:25:45Z"
  name: astracontrol-service-account
  namespace: default
  resourceVersion: "2767069"
  uid: 2ce068c4-810e-4a96-ada3-49cbf9ec3f89
secrets:
- name: astracontrol-service-account-dockercfg-48xhx
<strong>- name: secret-astracontrol-service-account</strong>
```

6. Enumere los secretos de la cuenta de servicio, reemplazando `<context>` con el contexto correcto para su instalación:

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

El final de la salida debe ser similar a lo siguiente:

```
"secrets": [
{ "name": "astracontrol-service-account-dockercfg-48xhx"},
{ "name": "secret-astracontrol-service-account"}
]
```

Los índices de cada elemento de la `secrets` la matriz comienza con 0. En el ejemplo anterior, el índice para `astracontrol-service-account-dockercfg-48xhx` sería 0 y el índice para `secret-astracontrol-service-account` sería 1. En la salida, anote el número de índice del secreto de la cuenta de servicio. Necesitará este número de índice en el siguiente paso.

7. Genere la kubeconfig de la siguiente manera:
   a. Cree un `create-kubeconfig.sh` archivo.
   b. Sustituya `TOKEN_INDEX` al principio de la secuencia de comandos siguiente con el valor correcto.

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

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

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

CONTEXT=$(kubectl config current-context)

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

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

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

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

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

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

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

# Set context to use token user
```

```
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --user ${CONTEXT}-${NAMESPACE}-token-
user

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

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

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

c. Origen de los comandos para aplicarlos al clúster de Kubernetes.

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

8. (Opcional) cambie el nombre de la Marca de prestigio por un nombre significativo para el clúster.

```
mv kubeconfig-sa YOUR_CLUSTER_NAME_kubeconfig
```

El futuro

Ahora que ha iniciado sesión y añadido un clúster a Astra Control, está listo para empezar a utilizar las funciones de gestión de datos de aplicaciones de Astra Control.

- "Inicie la gestión de aplicaciones"
- "Proteja sus aplicaciones"
- "Clone aplicaciones"
- "Configurar facturación"
- "Invitar y administrar usuarios"
- "Gestione las credenciales del proveedor de cloud"
- "Gestionar notificaciones"
- "Pon en marcha una instancia autogestionada de Astra Control"

Vídeos de Astra Control Service

Echa un vistazo a NetApp TV para obtener el contenido más reciente en vídeo, sobre Astra Control Service. NetApp TV incluye vídeos que muestran determinadas funciones

de Astra Control Service o cómo completar ciertas tareas comunes.

"Vídeos de Astra Control Service"

Conceptos

Arquitectura y componentes

Astra Control es una solución de gestión del ciclo de vida de los datos de aplicaciones de Kubernetes que simplifica las operaciones de aplicaciones con estado y te ayuda a almacenar, proteger y mover tus cargas de trabajo de Kubernetes entre entornos híbridos y multinube.

Funcionalidades

Astra Control ofrece funcionalidades cruciales para la gestión del ciclo de vida de los datos de las aplicaciones Kubernetes:

Tienda:

- Aprovisionamiento de almacenamiento dinámico para cargas de trabajo en contenedores
- Cifrado de datos en tránsito desde contenedores a volúmenes persistentes
- Replicación entre regiones y zonas

Proteger:

- Detección automatizada y protección compatible con las aplicaciones de toda una aplicación y sus datos
- Recuperación instantánea de una aplicación desde cualquier versión de snapshot según las necesidades de su organización
- Rápida recuperación tras fallos entre zonas, regiones y proveedores de cloud

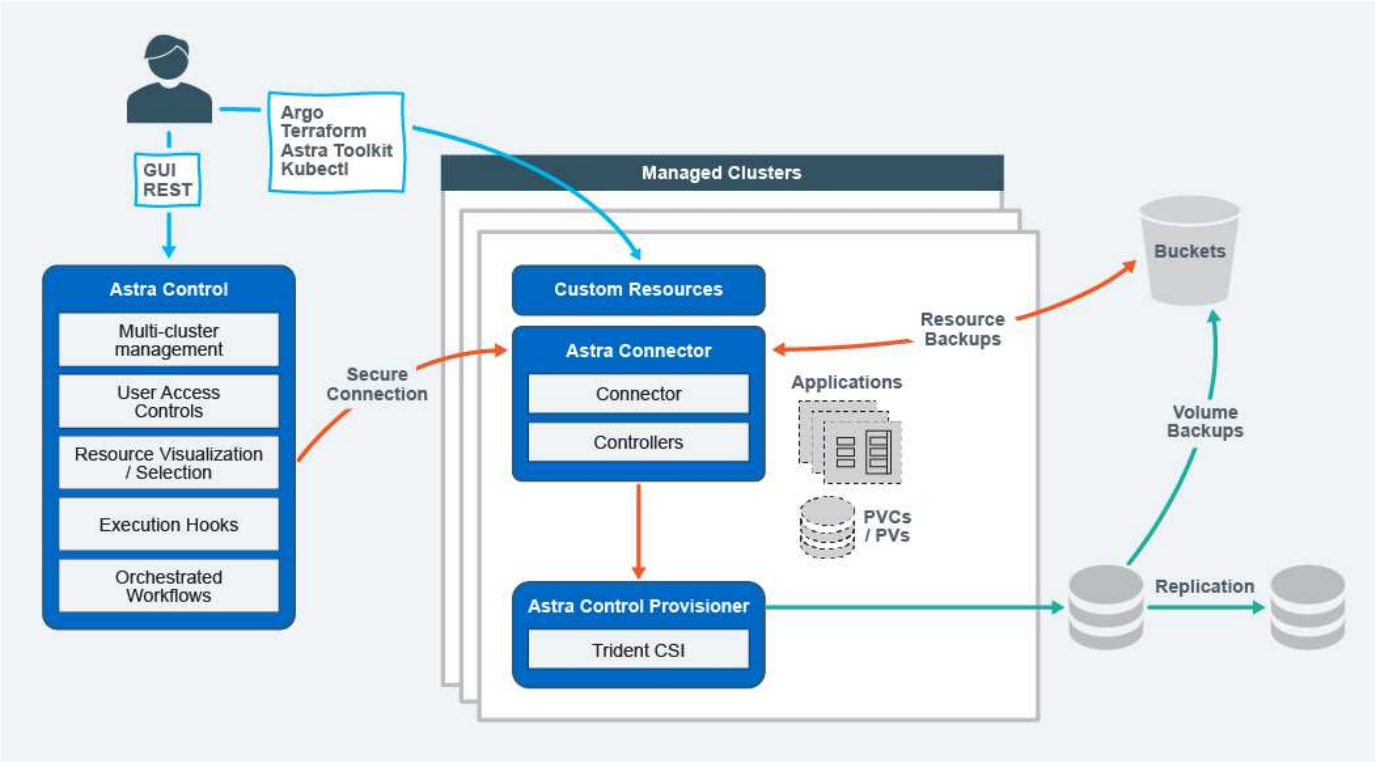
Mover:

- Completa movilidad de aplicaciones y datos en y entre clústeres y clouds de Kubernetes
- Clones instantáneos de aplicaciones y datos completos
- Migración de aplicaciones con un solo clic a través de una API e IU web consistentes

Arquitectura

La arquitectura de Astra Control permite que los departamentos de tecnología proporcionen funcionalidades de gestión de datos avanzadas que mejoran tanto la funcionalidad como la disponibilidad de las aplicaciones de Kubernetes, simplifica la gestión, la protección y el movimiento de cargas de trabajo en contenedores entre clouds públicos y entornos en las instalaciones. y proporciona funcionalidades de automatización a través de su API de REST y SDK, lo que permite un acceso mediante programación para una integración perfecta con los flujos de trabajo existentes.

Astra Control es nativo de Kubernetes, lo que permite flujos de trabajo de protección de datos que utilizan recursos personalizados y siguen siendo compatibles con las API y el SDK existentes. La protección de datos nativa de Kubernetes ofrece importantes ventajas; al integrarse sin problemas con las API y los recursos de Kubernetes, la protección de datos puede convertirse en una parte inherente del ciclo de vida de la aplicación mediante las herramientas GitOps o CI/CD existentes de una organización.



Astra Control se basa en cuatro componentes complementarios:

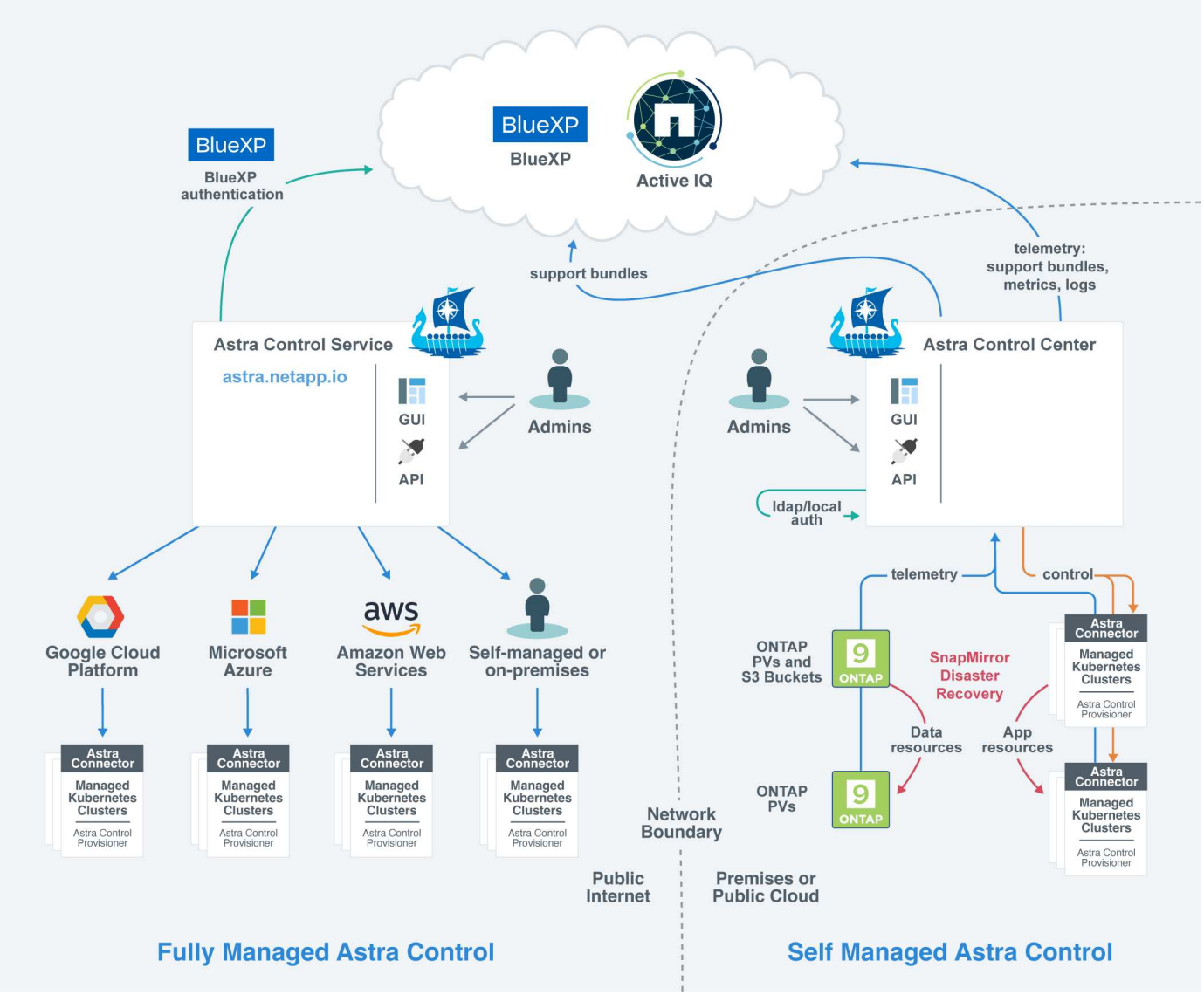
- **Astra Control**: Astra Control es el servicio de gestión centralizado para todos los clústeres gestionados, proporcionando cargas de trabajo orquestadas para la protección y movilidad de aplicaciones en la nube y on-premises, así como las siguientes capacidades:
  - Vista combinada de varios clústeres y clouds
  - Protección de flujos de trabajo orquestados
  - Visualización y selección granular de recursos
- **Astra Connector**: Astra Connector cuenta con Astra Control para proporcionar una conexión segura a cada clúster gestionado, ofreciendo la ejecución local de las operaciones programadas independientemente del estado de conexión, así como las siguientes capacidades:
  - Ejecución local de operaciones programadas independientemente del estado de conexión
  - Operaciones locales que distribuyen y optimizan el uso de los recursos del sistema de Astra en todos los clústeres
  - Instalación local que permite el acceso con menos privilegios al clúster para mejorar la seguridad
- **Astra Control Provisionador**: Astra Control Provisionador ofrece funcionalidad de aprovisionamiento CSI central y capacidades avanzadas de administración de almacenamiento para una mayor configuración de seguridad y recuperación ante desastres, así como las siguientes capacidades:
  - Aprovisionamiento de almacenamiento dinámico para cargas de trabajo en contenedores
  - Gestión de almacenamiento avanzada:
    - Cifrado en tránsito de datos desde contenedor a VP
    - Funcionalidad de SnapMirror Cloud con replicación entre zonas y regiones
- **Recursos personalizados de Astra**: Los recursos personalizados utilizados en cada clúster proporcionan un enfoque nativo de Kubernetes para ejecutar las operaciones localmente, simplificando la integración con otras herramientas y automatización compatibles con Kubernetes, además de proporcionar las

siguientes capacidades:

- Integración directa de herramientas del ecosistema y flujos de trabajo de automatización
- Primitivos de nivel inferior que permiten flujos de trabajo personalizados

Modelos de puesta en marcha

Astra Control está disponible en dos modelos de puesta en marcha.



- **Astra Control Service**: Un servicio gestionado por NetApp que proporciona gestión de datos para aplicaciones de clústeres de Kubernetes en varios entornos de proveedores de cloud, así como clústeres de Kubernetes autogestionados.

  "Documentación de Astra Control Service"

- **Astra Control Center**: Software autogestionado que proporciona gestión de datos para aplicaciones de clústeres de Kubernetes que se ejecutan en su entorno local. Astra Control Center también se puede instalar en entornos de varios proveedores de cloud con un entorno de administración del almacenamiento Cloud Volumes ONTAP de NetApp.

  "Documentación de Astra Control Center"

	Servicio de control Astra	Astra Control Center
¿Cómo se ofrece?	Como un servicio cloud totalmente gestionado de NetApp	Como software que se puede descargar, instalar y gestionar
¿Dónde está alojado?	En un cloud público que elija NetApp	En su propio clúster de Kubernetes
¿Cómo se actualiza?	Gestionado por NetApp	Usted administra cualquier actualización
¿Cuáles son las distribuciones de Kubernetes compatibles?	• * Proveedores en la nube* ◦ Amazon Web Services ▪ Amazon Elastic Kubernetes Service (EKS) ◦ Google Cloud ▪ Google Kubernetes Engine (GKE) ◦ Microsoft Azure ▪ Azure Kubernetes Service (AKS) • **Clusters autogestionados** ◦ Kubernetes (ascendente) ◦ Motor Kubernetes de rancher (RKE) ◦ OpenShift Container Platform de Red Hat • * Clústeres locales* ◦ Red Hat OpenShift Container Platform en las instalaciones	• Azure Kubernetes Service en HCI de pila de Azure • Anthos de Google • Kubernetes (ascendente) • Motor Kubernetes de rancher (RKE) • OpenShift Container Platform de Red Hat

	Servicio de control Astra	Astra Control Center
¿Cuáles son los back-ends de almacenamiento compatibles?	• * Proveedores en la nube* ◦ Amazon Web Services ▪ Amazon EBS ▪ Amazon FSX para ONTAP de NetApp ▪ "Cloud Volumes ONTAP" ◦ Google Cloud ▪ Disco persistente de Google ▪ Cloud Volumes Service de NetApp ▪ "Cloud Volumes ONTAP" ◦ Microsoft Azure ▪ Discos gestionados de Azure ▪ Azure NetApp Files ▪ "Cloud Volumes ONTAP" • **Clusters autogestionados** ◦ Amazon EBS ◦ Discos gestionados de Azure ◦ Disco persistente de Google ◦ "Cloud Volumes ONTAP" ◦ NetApp MetroCluster ◦ "El Longhorn" • * Clústeres locales* ◦ NetApp MetroCluster ◦ Sistemas ONTAP AFF y FAS de NetApp ◦ ONTAP Select de NetApp ◦ "Cloud Volumes ONTAP" ◦ "El Longhorn"	• Sistemas ONTAP AFF y FAS de NetApp • ONTAP Select de NetApp • "Cloud Volumes ONTAP" • "El Longhorn"

Si quiere más información

- "Documentación de Astra Control Service"
- "Documentación de Astra Control Center"
- "Documentación de Astra Trident"
- "API de control Astra"
- "Documentación de Cloud Insights"

- "Documentación de ONTAP"

Protección de datos

Conozca los tipos de protección de datos disponibles en Astra Control Service y cómo usarlos de la mejor forma para proteger sus aplicaciones.

Snapshot, backups y políticas de protección

Tanto Snapshot como los backups protegen los siguientes tipos de datos:

- La propia aplicación
- Todos los volúmenes de datos persistentes asociados con la aplicación
- Cualquier objeto de recurso que pertenezca a la aplicación

Un *snapshot* es una copia puntual de una aplicación que se almacena en el mismo volumen aprovisionado que la aplicación. Por lo general son rápidas. Es posible usar snapshots locales para restaurar la aplicación a un momento específico anterior. Las copias Snapshot son útiles para los clones rápidos; las copias Snapshot incluyen todos los objetos de Kubernetes para la aplicación, incluidos los archivos de configuración. Las copias Snapshot son útiles para clonar o restaurar una aplicación dentro del mismo clúster.

Un *backup* se basa en una instantánea. Se almacena en el almacén de objetos externo y, debido a esto, puede tardar más en hacerse en comparación con las copias Snapshot locales. Puede restaurar una copia de seguridad de aplicaciones en el mismo clúster, o puede migrar una aplicación restaurando su copia de seguridad en un clúster diferente. También es posible elegir un período de retención más largo para backups. Debido a que están almacenados en el almacén de objetos externo, los backups generalmente ofrecen mejor protección que las copias Snapshot en caso de fallo del servidor o pérdida de datos.

Una *política de protección* es una forma de proteger una aplicación mediante la creación automática de instantáneas, copias de seguridad o ambas de acuerdo con un programa definido para esa aplicación. Una política de protección también permite elegir cuántas Snapshot y backups se retendrán en la programación, y establecer diferentes niveles de granularidad de programación. Automatizar los backups y las copias Snapshot con una política de protección es la mejor forma de garantizar que cada aplicación esté protegida en función de las necesidades de la organización y los requisitos del acuerdo de nivel de servicio.

> *no puede estar completamente protegido hasta que tenga una copia de seguridad* reciente. Esto es importante porque los backups se almacenan en un almacén de objetos lejos de los volúmenes persistentes. Si un fallo o accidente limpia el cluster y su almacenamiento persistente asociado, necesitará una copia de seguridad para recuperar. Una Snapshot no le permite recuperar.

> Si realiza una copia de Snapshot o una copia de seguridad, pero se produce un error en la operación con el mensaje "no se ha creado el recurso debido a un problema de servidor interno", compruebe que el backend de almacenamiento que está utilizando tiene instalados los controladores correctos. Algunos back-ends de almacenamiento necesitan controladores de interfaz de almacenamiento de contenedores (CSI), mientras que otros necesitan una controladora de snapshots externa.

Backups inmutables

Un backup inmutable es un backup que no se puede cambiar ni eliminar durante un periodo determinado.

Cuando creas un backup inmutable, Astra Control realiza una comprobación para garantizar que el bloque que utilizas sea un bloque de escritura única y lectura múltiple (WORM), y, si es así, garantiza que el backup sea inmutable desde Astra Control.
Astra Control Service admite la creación de backups inmutables con las siguientes plataformas y tipos de bloques:

- Amazon Web Services con un bucket de Amazon S3 con S3 Object Lock configurado
- Microsoft Azure mediante un bucket de Azure con una política de retención configurada
- Google Kubernetes Engine (GKE) mediante un depósito de Google Cloud Storage con una política de retención configurada
- NetApp StorageGRID con un bloque de S3 con bloqueo de objetos de S3 GB configurado

Tenga en cuenta lo siguiente cuando trabaje con copias de seguridad inmutables:

- Si realiza la copia de SEGURIDAD en un bloque WORM en una plataforma no compatible o en un tipo de bloque no compatible, puede obtener resultados impredecibles, como un error en la eliminación de backups, incluso si ha transcurrido el tiempo de retención.
- Astra Control no admite políticas de gestión del ciclo de vida de los datos ni la eliminación manual de objetos en los bloques que utilizas con backups inmutables. Asegúrate de que el back-end de almacenamiento no esté configurado para gestionar el ciclo de vida de las copias Snapshot de Astra Control o de los datos que se han realizado backups.

Clones

Un *clone* es un duplicado exacto de una aplicación, su configuración y sus volúmenes de datos persistentes. Es posible crear manualmente un clon en el mismo clúster de Kubernetes o en otro clúster. El clonado de una aplicación puede ser útil si necesita mover aplicaciones y almacenamiento de un clúster de Kubernetes a otro.

Tipos de almacenamiento y rendimiento para clústeres de AWS

Astra Control Service puede usar Amazon Elastic Block Store (EBS), Amazon FSx para NetApp ONTAP o NetApp Cloud Volumes ONTAP como back-end de almacenamiento para los clústeres de Amazon Elastic Kubernetes Service (EKS).

Elastic Block Store (EBS) de Amazon

Los clústeres pueden utilizar controladores de interfaz de almacenamiento de contenedores (CSI) para interactuar con EBS. Cuando utiliza EBS como back-end de almacenamiento para clústeres EKS, puede configurar algunos parámetros de clase de almacenamiento. Para obtener más información acerca de qué significan los parámetros y cómo configurarlos, consulte "La documentación de Kubernetes".

Es posible usar varios tipos distintos de volúmenes con EBS:

- Unidades de estado sólido (SSD)
- Unidades de disco duro (HDD)
- Generación anterior

Para obtener más información sobre cada tipo de volumen y su rendimiento, consulte "La documentación de Amazon EBS". Para obtener información sobre precios, consulte "Precios de Amazon EBS".

Amazon FSX para ONTAP de NetApp

Cuando utiliza FSX para ONTAP de NetApp como back-end de almacenamiento para los clústeres de AWS, el rendimiento de I/o depende de la configuración del sistema de archivos y las características de sus cargas de trabajo. Para obtener información específica sobre el rendimiento de ONTAP de NetApp en FSX, consulte "Rendimiento de Amazon FSX para ONTAP de NetApp". Para obtener información sobre precios, consulte "Precios de Amazon FSX para ONTAP de NetApp".

Cloud Volumes ONTAP de NetApp

Para obtener información específica sobre la configuración de Cloud Volumes ONTAP de NetApp, incluidas las recomendaciones de rendimiento, visite "Documentación de Cloud Volumes ONTAP de NetApp".

Clases de almacenamiento y tamaño VP para clústeres AKS

Astra Control Service admite Azure NetApp Files, discos gestionados de Azure, o NetApp Cloud Volumes ONTAP como back-end de almacenamiento para los clústeres de Azure Kubernetes Service (AKS).

Azure NetApp Files

Astra Control Service es compatible con Azure NetApp Files como back-end de almacenamiento para los clústeres de Azure Kubernetes Service (AKS). Es necesario comprender cómo elegir una clase de almacenamiento y un tamaño de volumen persistente puede ayudarle a cumplir sus objetivos de rendimiento.

Niveles de servicio y clases de almacenamiento

Azure NetApp Files admite tres niveles de servicio: Almacenamiento Ultra, almacenamiento Premium y almacenamiento estándar. Cada uno de estos niveles de servicio está diseñado para satisfacer distintas necesidades de rendimiento:

Ultraespacio de almacenamiento
: Proporciona hasta 128 MIB/s de rendimiento por 1 TIB.

Almacenamiento excepcional
: Proporciona hasta 64 MIB/s de rendimiento por 1 TIB.

Almacenamiento estándar
: Proporciona hasta 16 MIB/s de rendimiento por 1 TIB.

Estos niveles de servicio son un atributo de un pool de capacidad. Es necesario configurar un pool de capacidad para cada nivel de servicio que se desea usar con los clústeres de Kubernetes. "Aprenda a configurar pools de capacidad".

El servicio Astra Control utiliza estos niveles de servicio como clases de almacenamiento para sus volúmenes persistentes. Cuando añade clústeres de Kubernetes a Astra Control Service, se le pedirá que elija Ultra, Premium o Standard como clase de almacenamiento predeterminada. Los nombres de los tipos de almacenamiento son *netapp-anf-perf-ultra*, *netapp-anf-perf-premium* y *netapp-anf-perf-standard*.

"Obtenga más información sobre estos niveles de servicio en los documentos de Azure NetApp Files".

Rendimiento y tamaño de volúmenes persistentes

Tal como se ha descrito anteriormente, el rendimiento de cada nivel de servicio es por 1 TIB de capacidad aprovisionada. Esto significa que los volúmenes de mayor tamaño proporcionan un mejor rendimiento. Por lo tanto, debe tener en cuenta tanto las necesidades de capacidad como el rendimiento al aprovisionar los volúmenes.

Tamaño de volumen mínimo

El servicio de control Astra aprovisiona volúmenes persistentes con un tamaño de volumen mínimo de 100 GIB, incluso si el PVC pide un tamaño de volumen menor. Por ejemplo, si la RVP de un gráfico Helm solicita 6 GIB, el Servicio de control Astra aprovisiona automáticamente un volumen de 100 GIB.

Backups de aplicaciones

Si realiza el backup de una aplicación que reside en el almacenamiento de Azure NetApp Files, el servicio Astra Control amplía automáticamente el pool de capacidad. Una vez finalizado el backup, el servicio Astra Control reduce el pool de capacidad a su tamaño anterior. En función de la suscripción a Azure, es posible que incurra en cargos de almacenamiento cuando esto ocurra. Se puede ver un historial de los eventos de cambio de tamaño del pool de capacidad en el registro de eventos de la página **Actividad**.

Si el pool de capacidad supera el tamaño máximo permitido por la suscripción a Azure durante la operación de cambio de tamaño, la operación de backup fallará y se activará una advertencia de la API de Azure.

Discos gestionados de Azure

Astra Control Service puede utilizar los controladores de interfaz de almacenamiento de contenedores (CSI) para interactuar con los discos administrados de Azure como back-end de almacenamiento. Este servicio proporciona almacenamiento a nivel de bloques gestionado por Azure.

"Obtenga más información acerca de los discos gestionados de Azure".

Cloud Volumes ONTAP de NetApp

Para obtener información específica sobre la configuración de Cloud Volumes ONTAP de NetApp, incluidas las recomendaciones de rendimiento, visite "Documentación de Cloud Volumes ONTAP de NetApp".

Tipo de servicio, clases de almacenamiento y tamaño VP para clústeres GKE

Astra Control Service es compatible con NetApp Cloud Volumes Service para Google Cloud, Google Persistent Disk o NetApp Cloud Volumes ONTAP como opciones de back-end de almacenamiento para los volúmenes persistentes.

Cloud Volumes Service para Google Cloud

Astra Control Service puede utilizar Cloud Volumes Service para Google Cloud como back-end de almacenamiento para volúmenes persistentes. Es necesario comprender cómo elegir un tipo de servicio, una clase de almacenamiento y un tamaño de volumen persistente pueden ayudarle a alcanzar sus objetivos de rendimiento.

Descripción general

Cloud Volumes Service for Google Cloud proporciona dos tipos de servicios: *CVS* y *CVS-Performance*. Estos tipos de servicio son compatibles con regiones específicas de Google Cloud. "Ve a los mapas de regiones globales de NetApp BlueXP" Para identificar el tipo de servicio compatible en la región de Google Cloud en la que residen los clústeres.

Si los clústeres de Kubernetes deben residir en una región específica, usará el tipo de servicio que se admite en esa región.

Sin embargo, si cuenta con flexibilidad para elegir entre regiones de Google Cloud, le recomendamos que siga estos requisitos de rendimiento:

- Para las aplicaciones K8S que tienen necesidades de almacenamiento de rendimiento de mediano a alto, elija una región de Google Cloud que admita CVS-Performance y use la clase de almacenamiento Premium o Extreme. Entre estas cargas de trabajo se incluyen las canalizaciones de IA/ML, las canalizaciones de CI/CD, el procesamiento de medios y las bases de datos, incluidas las bases de datos relacionales, NoSQL, series temporales, etc.
- Para las aplicaciones K8S que tienen necesidades de rendimiento del almacenamiento bajas o medianas (aplicaciones web, almacenamiento de archivos de uso general, etc.), elija una región de Google Cloud que admita CVS o CVS-Performance, con la clase de almacenamiento estándar.

> Si usa el tipo de servicio CVS con Astra Control Provisioner, debe configurar los pools de almacenamiento para poder aprovisionar volúmenes. Si se aprovisionan volúmenes sin pools de almacenamiento configurados, se producirá un error en el aprovisionamiento de volúmenes. Consulte la "Documentación de Cloud Volumes Service" para obtener más información sobre la creación de volúmenes.

La tabla siguiente proporciona una comparación rápida de la información descrita en esta página.

Tipo de servicio	Caso de uso	Regiones admitidas	Clases de almacenamiento	Tamaño mínimo del volumen
CVS-Performance	Con necesidades de rendimiento del almacenamiento medias o altas	"Consulte las regiones de Google Cloud admitidas."	• netapp-cvs-perf-standard • netapp-cvs-perf-premium • netapp-cvs-perf-extreme	100 GIB
CVS	Con necesidades de rendimiento del almacenamiento reducidas a medianas	"Consulte las regiones de Google Cloud admitidas."	netapp-cvs-standard	300 GIB

Tipo de servicio CVS-Performance

Obtenga más información sobre el tipo de servicio CVS-Performance antes de elegir una clase de almacenamiento y crear volúmenes persistentes.

Clases de almacenamiento

El tipo de servicio CVS-Performance es compatible con tres niveles de servicio: Standard, Premium y Extreme. Cuando añada un clúster a Astra Control Service, se le pedirá que elija Standard, Premium o Extreme como clase de almacenamiento predeterminada para volúmenes persistentes. Cada uno de estos niveles de servicio está diseñado para satisfacer distintas necesidades de capacidad y ancho de banda.

Los nombres de los tipos de almacenamiento son *netapp-cvs-perf-standard*, *netapp-cvs-perf-premium* y *netapp-cvs-perf-extreme*.

"Obtenga más información sobre estos niveles de servicio en los documentos de Cloud Volumes Service para Google Cloud".

Rendimiento y tamaño de volúmenes persistentes

"Como explican los documentos de Google Cloud", el ancho de banda permitido para cada nivel de servicio es por GIB de capacidad aprovisionada. Esto significa que los volúmenes más grandes proporcionarán un mejor rendimiento.

Asegúrese de leer la página de Google Cloud vinculada a la anterior. Incluye comparaciones de costes y ejemplos que pueden ayudarle a comprender mejor cómo combinar un nivel de servicio con el tamaño del volumen para cumplir sus objetivos de rendimiento.

Tamaño de volumen mínimo

Astra Control Service aprovisiona volúmenes persistentes mediante un tamaño de volumen mínimo de 100 GIB con el tipo de servicio CVS-Performance, incluso si la RVP solicita un tamaño de volumen menor. Por ejemplo, si la RVP de un gráfico Helm solicita 6 GIB, el Servicio de control Astra aprovisiona automáticamente un volumen de 100 GIB.

Tipo de servicio CVS

Obtenga más información sobre el tipo de servicio CVS antes de elegir una clase de almacenamiento y crear volúmenes persistentes.

Clase de almacenamiento

Se admite un nivel de servicio con el tipo de servicio CVS: Standard. Cuando se gestionan clústeres en regiones donde se admite el tipo de servicio CVS, Astra Control Service utiliza el nivel de servicio estándar como clase de almacenamiento predeterminada para volúmenes persistentes. La clase de almacenamiento recibe el nombre de *netapp-cvs-Standard*.

"Obtenga más información acerca del nivel de servicio estándar en los documentos de Cloud Volumes Service para Google Cloud".

Rendimiento y tamaño de volúmenes persistentes

El ancho de banda permitido para el tipo de servicio CVS es por GIB de capacidad aprovisionada. Esto significa que los volúmenes más grandes proporcionarán un mejor rendimiento.

Tamaño de volumen mínimo

Astra Control Service aprovisiona volúmenes persistentes utilizando un tamaño de volumen mínimo de 300 GIB con el tipo de servicio CVS, incluso si el PVC pide un tamaño de volumen menor. Por ejemplo, si se solicitan 20 GIB, Astra Control Service aprovisiona automáticamente un volumen de 300 GIB.

Debido a una limitación, si una RVP solicita un volumen entre 700-999 GIB, Astra Control Service aprovisiona automáticamente un tamaño de volumen de 1000 GIB.

Disco persistente de Google

Astra Control Service puede utilizar controladores de interfaz de almacenamiento de contenedores (CSI) para interactuar con Google Persistent Disk como back-end de almacenamiento. Este servicio proporciona almacenamiento en el nivel de bloques gestionado por Google.

"Obtenga más información acerca de Google Persistent Disk".

"Obtenga más información sobre los diferentes niveles de rendimiento de los discos persistentes de Google".

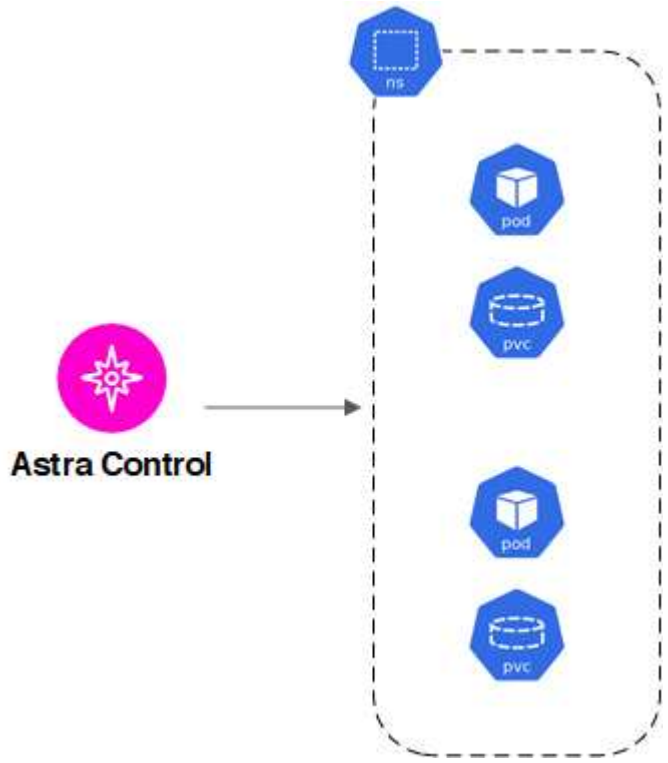
Cloud Volumes ONTAP de NetApp

Para obtener información específica sobre la configuración de Cloud Volumes ONTAP de NetApp, incluidas las recomendaciones de rendimiento, visite "Documentación de Cloud Volumes ONTAP de NetApp".

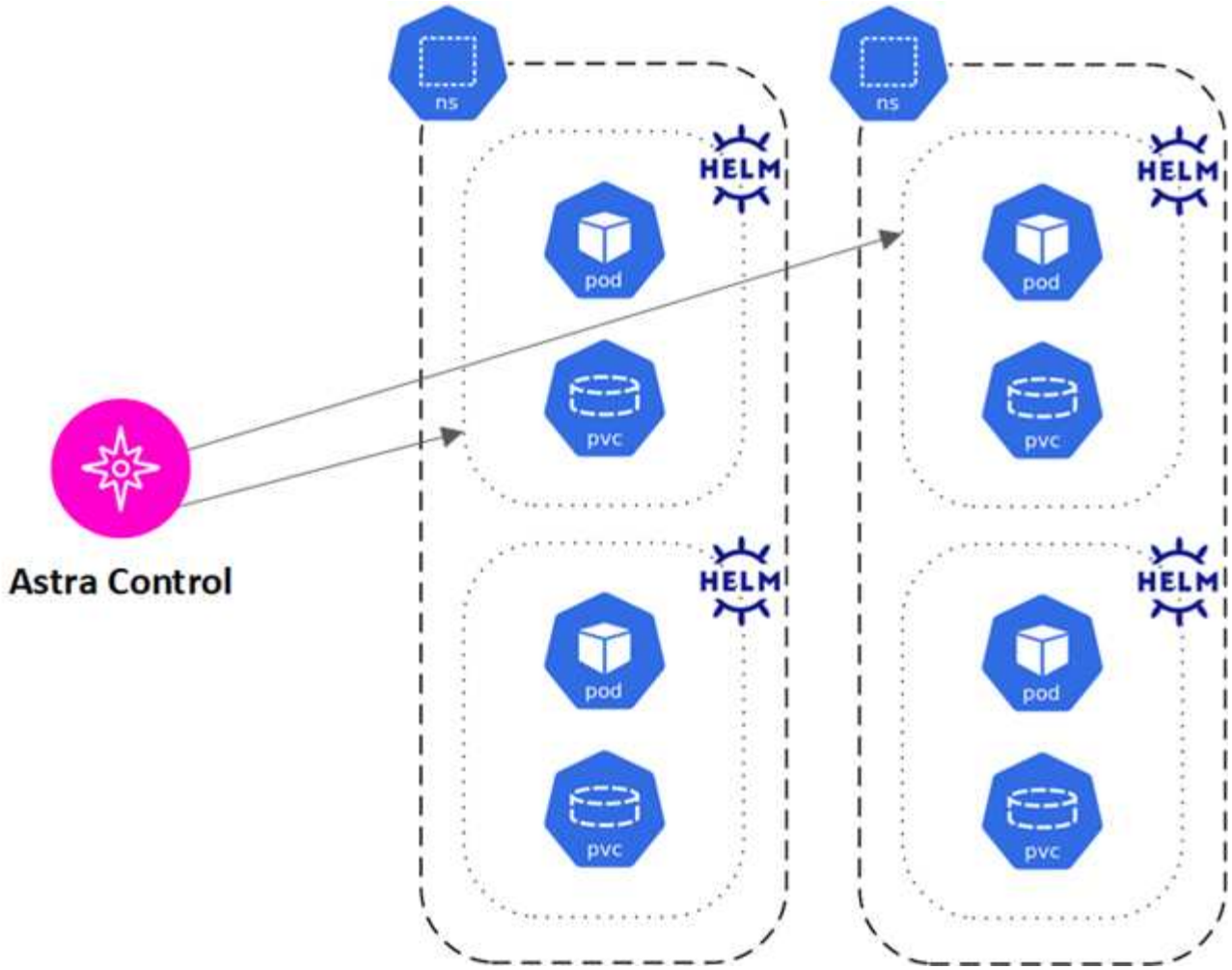
Gestión de aplicaciones

Cuando Astra Control detecta sus clústeres, las aplicaciones de esos clústeres no se gestionan hasta que elija cómo desea gestionarlas. Una aplicación administrada de Astra Control puede ser cualquiera de las siguientes:

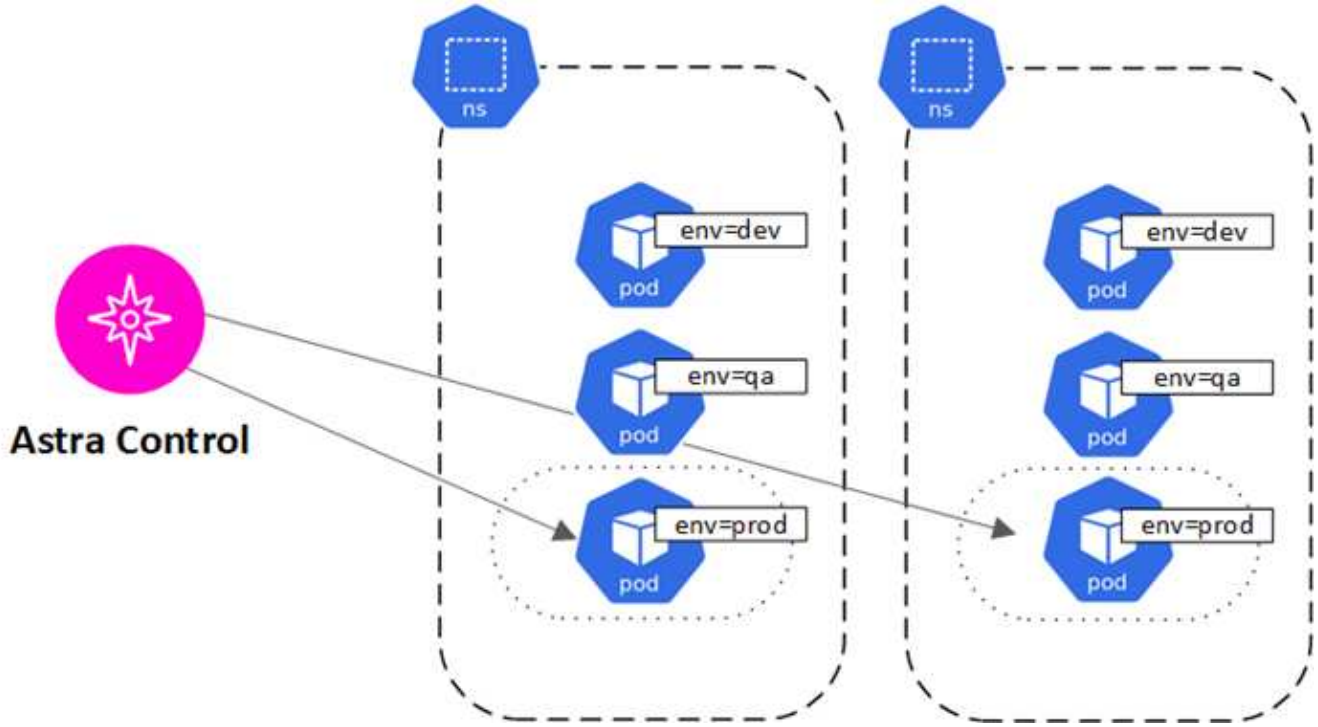
- Un espacio de nombres, incluidos todos los recursos de ese espacio de nombres



- Una aplicación individual implementada en uno o más espacios de nombres (se utiliza Helm 3 en este ejemplo)



- Un grupo de recursos que se identifica con una etiqueta de Kubernetes dentro de uno o varios espacios de nombres



Roles de usuario y espacios de nombres

Obtenga información acerca de las funciones de usuario y los espacios de nombres en Astra Control y cómo puede utilizarlas para controlar el acceso a los recursos de la organización.

Roles de usuario

Puede utilizar las funciones para controlar el acceso de los usuarios a los recursos o capacidades de Astra Control. Las siguientes son las funciones de usuario de Astra Control:

- Un **propietario** tiene permisos de administrador y puede eliminar cuentas.
- Un **Admin** tiene permisos de miembro y puede invitar a otros usuarios.
- Un **Miembro** puede administrar completamente aplicaciones y clústeres.
- Un **Visor** puede ver los recursos.

Puede agregar restricciones a un usuario Miembro o Visor para restringir el usuario a uno o más Espacios de nombres.

Espacios de nombres

Un espacio de nombres es un ámbito que puede asignar a recursos específicos de un clúster gestionado por Astra Control. Astra Control detecta los espacios de nombres de un clúster cuando agrega el clúster a Astra Control. Una vez detectados, los espacios de nombres están disponibles para asignarlos como restricciones a los usuarios. Sólo los miembros que tienen acceso a ese espacio de nombres pueden usar ese recurso. Puede utilizar espacios de nombres para controlar el acceso a los recursos mediante un paradigma que tenga sentido para la organización; por ejemplo, por regiones físicas o divisiones dentro de una empresa. Cuando agrega restricciones a un usuario, puede configurarlo para que tenga acceso a todos los espacios de nombres o sólo a un conjunto específico de espacios de nombres. También es posible asignar restricciones de espacio de nombres usando etiquetas de espacio de nombres.

Obtenga más información

- "Gestionar roles"

Utilice el servicio Astra Control Service

Inicie sesión en el servicio Astra Control

Se puede acceder al servicio Astra Control mediante una interfaz de usuario basada en SaaS https://astra.netapp.io.

> Puede utilizar el inicio de sesión único para iniciar sesión con credenciales del directorio corporativo (identidad federada). Para obtener más información, visite la "Centro de ayuda" Y, a continuación, seleccione **Opciones de inicio de sesión de Cloud Central**.

Antes de empezar

- "Un ID de usuario de BlueXP".
- "Una nueva cuenta de Astra Control" o. "una invitación a una cuenta existente".
- Un navegador web compatible.

  Astra Control Service es compatible con las versiones recientes de Firefox, Safari y Chrome con una resolución mínima de 1280 x 720.

Pasos

1. Abra un explorador web y vaya a. https://astra.netapp.io.
2. Inicia sesión con tus credenciales de NetApp BlueXP.

Gestione y proteja aplicaciones

Inicie la gestión de aplicaciones

Usted primero "Añada un clúster de Kubernetes a Astra Control", Puede instalar aplicaciones en el clúster (fuera de Astra Control) y, a continuación, ir a la página aplicaciones de Astra Control para definir las aplicaciones.

Puede definir y gestionar aplicaciones que incluyan recursos de almacenamiento con pods en ejecución o aplicaciones que incluyan recursos de almacenamiento sin ningún pods en ejecución. Las aplicaciones que no tienen pods en ejecución se conocen como aplicaciones de solo datos.

Requisitos de gestión de aplicaciones

Astra Control tiene los siguientes requisitos de gestión de aplicaciones:

- **Licencias**: Para administrar más de 10 espacios de nombres, necesitas una suscripción a Astra Control.
- **Namespaces**: Las aplicaciones se pueden definir dentro de uno o más espacios de nombres especificados en un único clúster mediante Astra Control. Una aplicación puede contener recursos que abarcan varios espacios de nombres dentro del mismo clúster. Astra Control no admite la capacidad de definir las aplicaciones en varios clústeres.
- **Clase de almacenamiento**: Si instala una aplicación con una clase de almacenamiento definida explícitamente y necesita clonar la aplicación, el clúster de destino para la operación de clonación debe tener la clase de almacenamiento especificada originalmente. Se producirá un error al clonar una

aplicación con una clase de almacenamiento definida explícitamente a un clúster que no tenga la misma clase de almacenamiento.

- **Recursos de Kubernetes**: Las aplicaciones que utilizan los recursos de Kubernetes no recopilados por Astra Control pueden no tener funciones completas de gestión de datos de aplicaciones. Astra Control recopila los siguientes recursos de Kubernetes:

`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`		

Métodos de instalación de aplicaciones compatibles

Astra Control es compatible con los siguientes métodos de instalación de aplicaciones:

- **Fichero manifiesto**: Astra Control admite aplicaciones instaladas desde un archivo manifiesto mediante kubectl. Por ejemplo:

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

- **Helm 3**: Si utiliza Helm para instalar aplicaciones, Astra Control requiere Helm versión 3. La gestión y clonación de aplicaciones instaladas con Helm 3 (o actualizadas de Helm 2 a Helm 3) son totalmente compatibles. No se admite la administración de aplicaciones instaladas con Helm 2.
- **Aplicaciones implementadas por el operador**: Astra Control admite aplicaciones instaladas con operadores de ámbito de espacio de nombres que, en general, están diseñados con una arquitectura de "paso por valor" en lugar de "paso por referencia". Un operador y la aplicación que instale deben usar el mismo espacio de nombres; es posible que deba modificar el archivo .yaml de despliegue para que el operador se asegure de que así sea.

  Las siguientes son algunas aplicaciones del operador que siguen estos patrones:

  - "Apache K8ssandra"

    > Para K8ssandra, se admiten operaciones de restauración in situ. Una operación de restauración a un nuevo espacio de nombres o clúster requiere que se apague la instancia original de la aplicación. Esto es para garantizar que la información del grupo de pares no conduzca a la comunicación entre instancias. No se admite la clonación de la aplicación.

  - "Jenkins CI"

- "Clúster Percona XtraDB"

Es posible que Astra Control no pueda clonar a un operador diseñado con una arquitectura "pase por referencia" (por ejemplo, el operador CockroachDB). Durante estos tipos de operaciones de clonado, el operador clonado intenta hacer referencia a los secretos de Kubernetes del operador de origen a pesar de tener su propio secreto nuevo como parte del proceso de clonado. Es posible que se produzca un error en la operación de clonado porque Astra Control no conoce los secretos de Kubernetes en el operador de origen.

Instale las aplicaciones en el clúster

La tienes "ha agregado el clúster" A Astra Control, puede instalar aplicaciones o gestionar las aplicaciones existentes en el clúster. Cualquier aplicación que se limita a uno o más espacios de nombres se puede gestionar.

Astra Control gestionará las aplicaciones con estado solo si el almacenamiento está en una clase de almacenamiento compatible con Astra Control. Astra Control Service es compatible con cualquier clase de almacenamiento que sea compatible con el aprovisionador de control Astra o un controlador CSI genérico.

- "Obtenga información sobre clases de almacenamiento para clústeres GKE"
- "Obtenga información sobre clases de almacenamiento para clústeres de AKS"
- "Obtenga información sobre las clases de almacenamiento para clústeres de AWS"

Defina las aplicaciones

Una vez que Astra Control detecta espacios de nombres en sus clústeres, puede definir las aplicaciones que desea administrar. Puede elegir administrar una aplicación que abarque uno o más espacios de nombres o. gestione un espacio de nombres completo como una única aplicación. Todo se reduce al nivel de granularidad que necesita para las operaciones de protección de datos.

Aunque Astra Control le permite gestionar por separado ambos niveles de la jerarquía (el espacio de nombres y las aplicaciones en ese espacio de nombres o espacio de nombres expansivo), la práctica recomendada es elegir uno u otro. Las acciones que realice en Astra Control pueden fallar si las acciones se llevan a cabo al mismo tiempo tanto en el espacio de nombres como en el nivel de la aplicación.

> A modo de ejemplo, puede que desee establecer una normativa de backup para «maria» con una cadencia semanal, pero es posible que deba realizar backups de «mariadb» (que se encuentra en el mismo espacio de nombres) con mayor frecuencia que esta. Según estas necesidades, debería gestionar las aplicaciones por separado, no como una aplicación de espacio de nombres único.

Antes de empezar

- Se añadió un clúster de Kubernetes a Astra Control.
- Una o más aplicaciones instaladas en el clúster. Obtenga más información sobre los métodos de instalación de aplicaciones compatibles.
- Espacios de nombres existentes en el clúster Kubernetes que se añadió a Astra Control.
- (Opcional) una etiqueta de Kubernetes en cualquiera "Recursos de Kubernetes compatibles".

Una etiqueta es una pareja clave/valor que se puede asignar a objetos de Kubernetes para su identificación. Las etiquetas facilitan la ordenación, la organización y la búsqueda de los objetos de Kubernetes. Para obtener más información acerca de las etiquetas de Kubernetes, "Consulte la documentación oficial de Kubernetes".

Acerca de esta tarea

- Antes de empezar, también debe entender "gestión de espacios de nombres estándar y del sistema".
- Si planea utilizar varios espacios de nombres con sus aplicaciones en Astra Control, tenga en cuenta "modificación de los roles de usuario con restricciones de espacio de nombres" antes de definir aplicaciones.
- Para obtener instrucciones sobre cómo gestionar aplicaciones mediante la API de Astra Control, consulte "Información sobre API y automatización de Astra".

Opciones de gestión de aplicaciones

- Defina los recursos que se van a administrar como una aplicación
- Defina un espacio de nombres para administrar como una aplicación

Defina los recursos que se van a administrar como una aplicación

Puede especificar el "Los recursos de Kubernetes forman una aplicación" Que desea gestionar con Astra Control. Definir una aplicación le permite agrupar elementos de su clúster de Kubernetes en una única aplicación. Esta colección de recursos de Kubernetes está organizada por criterios de espacio de nombres y selector de etiquetas.

Definir una aplicación le proporciona un control más granular de lo que se debe incluir en una operación Astra Control, que incluye clonado, copias Snapshot y backups.

Al definir aplicaciones, asegúrese de no incluir un recurso de Kubernetes en varias aplicaciones con políticas de protección. La superposición de políticas de protección en recursos de Kubernetes puede provocar conflictos de datos.

Obtenga más información sobre la adición de recursos con ámbito de clúster a los espacios de nombres de la aplicación.

Puede importar recursos de clúster asociados a los recursos de espacio de nombres además de los que se incluyen automáticamente Astra Control. Puede agregar una regla que incluirá recursos de un grupo específico, tipo, versión y, opcionalmente, etiqueta. Es posible que desee hacer esto si hay recursos que Astra Control no incluye automáticamente.

No puede excluir ninguno de los recursos con ámbito de clúster que Astra Control incluya automáticamente.

Puede agregar lo siguiente `apiVersions` (Que son los grupos combinados con la versión API):

Tipo de recursos	ApiVersions (grupo + versión)
`ClusterRole`	rbac.authorization.k8s.io/v1
`ClusterRoleBinding`	rbac.authorization.k8s.io/v1
`CustomResource`	apiextensions.k8s.io/v1, apiextensions.k8s.io/v1beta1
`CustomResourceDefinition`	apiextensions.k8s.io/v1, apiextensions.k8s.io/v1beta1
`MutatingWebhookConfiguration`	admissionregistration.k8s.io/v1
`ValidatingWebhookConfiguration`	admissionregistration.k8s.io/v1

Pasos

1. En la página aplicaciones, seleccione **definir**.
2. En la ventana **definir aplicación**, introduzca el nombre de la aplicación.
3. Seleccione el clúster en el que se ejecuta la aplicación en la lista desplegable **Cluster**.
4. Elija un espacio de nombres para su aplicación en la lista desplegable **espacio de nombres**.

> Las aplicaciones se pueden definir dentro de uno o más espacios de nombres especificados en un único clúster mediante Astra Control. Una aplicación puede contener recursos que abarcan varios espacios de nombres dentro del mismo clúster. Astra Control no admite la capacidad de definir las aplicaciones en varios clústeres.

5. (Opcional) Introduzca una etiqueta para los recursos de Kubernetes en cada espacio de nombres. Puede especificar una sola etiqueta o un criterio de selector de etiquetas (consulta).

> Para obtener más información acerca de las etiquetas de Kubernetes, "Consulte la documentación oficial de Kubernetes".

6. (Opcional) Añada espacios de nombres adicionales para la aplicación seleccionando **Agregar espacio de nombres** y eligiendo el espacio de nombres en la lista desplegable.
7. (Opcional) Introduzca los criterios de etiqueta única o selector de etiquetas para los espacios de nombres adicionales que añada.
8. (Opcional) para incluir recursos de ámbito de clúster además de los que Astra Control incluye

automáticamente, marque **incluir recursos adicionales de ámbito de clúster** y complete lo siguiente:

a. Seleccione **Agregar regla de inclusión**.

b. **Grupo**: En la lista desplegable, seleccione el grupo API de recursos.

c. **Kind**: En la lista desplegable, seleccione el nombre del esquema de objetos.

d. **Versión**: Introduzca la versión API.

e. **Selector de etiquetas**: Opcionalmente, incluya una etiqueta que se agregará a la regla. Esta etiqueta se utiliza para recuperar solo los recursos que coincidan con esta etiqueta. Si no proporciona una etiqueta, Astra Control recopila todas las instancias del tipo de recurso especificado para ese clúster.

f. Revise la regla que se crea en función de las entradas.

g. Seleccione **Agregar**.

> Puede crear tantas reglas de recursos con ámbito de clúster como desee. Las reglas aparecen en definir resumen de la aplicación.

9. Seleccione **definir**.
10. Después de seleccionar **definir**, repita el proceso para otras aplicaciones, según sea necesario.

Cuando termine de definir una aplicación, la aplicación aparecerá en `Healthy` estado en la lista de aplicaciones de la página aplicaciones. Ahora puede clonarla y crear backups y copias Snapshot.

> Es posible que la aplicación que acaba de agregar tenga un icono de advertencia en la columna protegido, lo que indica que no se ha realizado una copia de seguridad y que aún no está programada para las copias de seguridad.

> Para ver los detalles de una aplicación en particular, seleccione el nombre de la aplicación.

Para ver los recursos agregados a esta aplicación, seleccione la ficha **Recursos**. Seleccione el número después del nombre del recurso en la columna Resource o introduzca el nombre del recurso en Search para ver los recursos adicionales con ámbito del clúster incluidos.

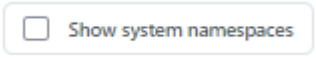
Defina un espacio de nombres para administrar como una aplicación

Puede añadir todos los recursos de Kubernetes en un espacio de nombres a la gestión de Astra Control al definir los recursos de ese espacio de nombres como una aplicación. Este método es preferible a definir las aplicaciones individualmente si lo hace "pretende gestionar y proteger todos los recursos de un espacio de nombres determinado" de manera similar y a intervalos comunes.

Pasos

1. En la página Clusters, seleccione un clúster.
2. Seleccione la ficha **Namespaces**.
3. Seleccione el menú acciones del espacio de nombres que contiene los recursos de aplicación que desea administrar y seleccione **definir como aplicación**.

> Si desea definir varias aplicaciones, seleccione en la lista de espacios de nombres y seleccione el botón **acciones** en la esquina superior izquierda y seleccione **definir como aplicación**. Esto definirá varias aplicaciones individuales en sus espacios de nombres individuales. Para aplicaciones con varios espacios de nombres, consulte Defina los recursos que se van a administrar como una aplicación.

Active la casilla de verificación **Mostrar espacios de nombres del sistema** para mostrar los espacios de nombres del sistema que normalmente no se usan en la administración de aplicaciones de forma predeterminada. 

"Leer más".

Una vez completado el proceso, las aplicaciones asociadas al espacio de nombres aparecen en la `Associated applications` columna.

[Vista PREVIA TÉCNICA] Defina una aplicación utilizando un recurso personalizado de Kubernetes

Puede especificar los recursos de Kubernetes que desee gestionar con Astra Control definiéndolos como aplicación mediante un recurso personalizado (CR). Puede añadir recursos de ámbito en clúster si desea gestionar esos recursos individualmente o todos los recursos de Kubernetes en un espacio de nombres si, por ejemplo, tiene la intención de gestionar y proteger todos los recursos de un espacio de nombres particular de una forma similar y con intervalos comunes.

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre (por ejemplo, `astra_mysql_app.yaml`).
2. Asigne un nombre a la aplicación en `metadata.name`.
3. Defina los recursos de aplicación que se van a gestionar:

spec.includedClusterScopedResources

Incluye los tipos de recursos de ámbito del clúster además de los que Astra Control incluye automáticamente:

- **spec.includedClusterScopedResources**: *(Opcional)* Una lista de tipos de recursos de ámbito de cluster que se incluirán.
  - **GroupVersionKind**: *(Opcional)* identifica inequívocamente un tipo.
    - **GROUP**: *(requerido si se usa groupVersionKind)* Grupo API del recurso a incluir.
    - **VERSIÓN**: *(requerido si se usa groupVersionKind)* Versión API del recurso a incluir.
    - **Kind**: *(requerido si se usa groupVersionKind)* tipo de recurso a incluir.
  - **LabelSelector**: *(Opcional)* Una consulta de etiqueta para un conjunto de recursos. Se utiliza para recuperar solo los recursos que coinciden con la etiqueta. Si no proporciona una etiqueta, Astra Control recopila todas las instancias del tipo de recurso especificado para ese clúster. El resultado de matchLabels y matchExpressions son ANDed.
    - **MatchLabels**: *(Opcional)* Un mapa de {key,value} pares. Un único {key,value} en el mapa matchLabels es equivalente a un elemento de matchExpressions que tiene un campo clave de “key”, operador como “in” y matriz de valores que contiene solo “value”. Los requisitos son ANDed.
    - **MatchExpressions**: *(Opcional)* Una lista de los requisitos del selector de etiquetas. Los requisitos son ANDed.
      - **KEY**: *(requerido si se usa matchExpressions)* La clave de etiqueta asociada con el selector de etiquetas.
      - **OPERATOR**: *(requerido si se usa matchExpressions)* representa la relación de una clave con un conjunto de valores. Los operadores válidos son `In`, `NotIn`, `Exists` y.. `DoesNotExist`.
      - **VALORES**: *(requerido si se utiliza matchExpressions)_Una matriz de valores de cadena. Si el operador es `In` o. `NotIn`, la matriz de valores debe _not* estar vacía. Si el operador es `Exists` o. `DoesNotExist`, la matriz de valores debe estar vacía.

spec.includedNamespaces

Incluya espacios de nombres y recursos dentro de esos recursos en la aplicación:

- **spec.includedNamespaces**: _(required)_Define el espacio de nombres y los filtros opcionales para la selección de recursos.
  - **Namespace**: *(required)* El espacio de nombres que contiene los recursos de la aplicación que desea administrar con Astra Control.
  - **LabelSelector**: *(Opcional)* Una consulta de etiqueta para un conjunto de recursos. Se utiliza para recuperar solo los recursos que coinciden con la etiqueta. Si no proporciona una etiqueta, Astra Control recopila todas las instancias del tipo de recurso especificado para ese clúster. El resultado de matchLabels y matchExpressions son ANDed.
    - **MatchLabels**: *(Opcional)* Un mapa de {key,value} pares. Un único {key,value} en el mapa matchLabels es equivalente a un elemento de matchExpressions que tiene un campo clave de “key”, operador como “in” y matriz de valores que contiene solo “value”. Los requisitos son ANDed.
    - **MatchExpressions**: *(Opcional)* Una lista de los requisitos del selector de etiquetas. `key` y.. `operator` son obligatorios. Los requisitos son ANDed.

- **KEY**: *(requerido si se usa matchExpressions)* La clave de etiqueta asociada con el selector de etiquetas.
- **OPERATOR**: *(requerido si se usa matchExpressions)* representa la relación de una clave con un conjunto de valores. Los operadores válidos son `In`, `NotIn`, `Exists` y.. `DoesNotExist`.
- **Valores**: *(requerido si se usa matchExpressions)* Una matriz de valores de cadena. Si el operador es `In` o. `NotIn`, la matriz de valores debe *not* estar vacía. Si el operador es `Exists` o. `DoesNotExist`, la matriz de valores debe estar vacía.

Ejemplo YAML:

```
apiVersion: astra.netapp.io/v1
kind: Application
metadata:
  name: astra_mysql_app
spec:
  includedNamespaces:
    - namespace: astra_mysql_app
      labelSelector:
        matchLabels:
          app: nginx
          env: production
        matchExpressions:
          - key: tier
            operator: In
            values:
              - frontend
              - backend
```

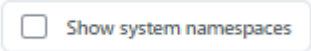
4. Después de rellenar el `astra_mysql_app.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -f astra_mysql_app.yaml -n astra-connector
```

¿Qué ocurre con los espacios de nombres del sistema?

Astra Control también detecta espacios de nombres de sistemas en un clúster de Kubernetes. No le mostramos estos espacios de nombres del sistema de forma predeterminada porque es raro que necesite realizar backups de los recursos de la aplicación del sistema.

Puede visualizar los espacios de nombres del sistema desde la ficha espacios de nombres de un clúster seleccionado activando la casilla de verificación **Mostrar espacios de nombres del sistema** .



Astra Control en sí no es una aplicación estándar; es una "aplicación del sistema". No debe intentar gestionar Astra Control por sí mismo. Astra Control no se muestra de forma predeterminada para la gestión.

Proteja las aplicaciones con snapshots y backups

Proteja sus aplicaciones tomando snapshots y backups usando una política de protección automatizada o de manera ad hoc. Puede utilizar la interfaz de usuario de Astra o. "La API de control Astra" para proteger aplicaciones.

Más información acerca de "Protección de datos en Astra Control".

Puede realizar las siguientes tareas relacionadas con la protección de los datos de la aplicación:

- Configure una política de protección
- Crear una copia de Snapshot
- Cree un backup
- Habilite el backup y la restauración para las operaciones económicas de ontap-nas
- Cree un backup inmutable
- Ver Snapshot y backups
- Eliminar snapshots
- Cancelar backups
- Eliminar backups

Configure una política de protección

La política de protección protege una aplicación mediante la creación de snapshots, backups o ambos con una programación definida. Puede optar por crear snapshots y backups por hora, día, semana y mes, y especificar la cantidad de copias que desea retener. Puede definir una política de protección con la interfaz de usuario web de Astra Control o un archivo de recursos personalizados (CR).

Si necesita que backups o snapshots se ejecuten con más frecuencia de una vez por hora, puede hacerlo "Utilice la API REST de Astra Control para crear copias Snapshot y copias de seguridad".

Si va a definir una política de protección que crea backups inmutables para escribir bloques WORM (escritura única y lectura múltiple), asegúrese de que el tiempo de retención de los backups no sea más corto que el período de retención configurado para el bloque.

Reajuste los programas de copia de seguridad y replicación para evitar superposiciones de programas. Por ejemplo, realice backups en la parte superior de la hora cada hora y programe la replicación para que comience con un desplazamiento de 5 minutos y un intervalo de 10 minutos.

Configure una política de protección con la interfaz de usuario web

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. Seleccione **Protección de datos**.
3. Seleccione **Configurar política de protección**.
4. Definir una programación de protección seleccionando la cantidad de Snapshot y backups que se deben mantener en las programaciones por hora, por día, por semana y por mes.

   Puede definir las programaciones por hora, por día, por semana y por mes de forma simultánea. Una programación no se activa hasta que se establece un nivel de retención.

   Al establecer un nivel de retención para backups, puede elegir el bloque en el que desea almacenar los backups.

   En el siguiente ejemplo, se establecen cuatro programaciones de protección: Por hora, día, semana y mes para las copias Snapshot y los backups.

   [Captura de pantalla de una directiva de configuración de ejemplo en la que puede elegir hacer Snapshots y backups cada hora, día, semana o mes.]

5. [**Vista previa tecnológica**] Elija un depósito de destino para las copias de seguridad o instantáneas de la lista de depósitos de almacenamiento.
6. Seleccione **Revisión**.
7. Seleccione **Configurar política de protección.**

[Tech preview] Configurar una política de protección con un CR

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre `astra-control-schedule-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tus necesidades de entorno de Astra Control, configuración del clúster y protección de datos:
   - <CR_NAME>: El nombre de este recurso personalizado; elija un nombre único y sensible para su entorno.
   - <APPLICATION_NAME>: El nombre de Kubernetes de la aplicación de la que se va a realizar el backup.
   - <APPVAULT_NAME>: El nombre del AppVault donde se debe almacenar el contenido de la copia de seguridad.
   - <BACKUPS_RETAINED>: La cantidad de backups que se retendrán. Cero indica que no se debe crear ningún backup.
   - <SNAPSHOTS_RETAINED>: La cantidad de snapshots que se retendrán. Cero indica que no se debe crear ninguna instantánea.
   - <GRANULARITY>: La frecuencia con la que debe ejecutarse la programación. Los posibles valores, junto con los campos asociados necesarios:
     - `hourly` (requiere que especifique `spec.minute`)
     - `daily` (requiere que especifique `spec.minute` y.. `spec.hour`)
     - `weekly` (requiere que especifique `spec.minute`, `spec.hour`, y. `spec.dayOfWeek`)

    - `monthly` (requiere que especifique `spec.minute`, `spec.hour`, y. `spec.dayOfMonth`)
  - <DAY_OF_MONTH>: *(Opcional)* el día del mes (1 - 31) en el que debe ejecutarse la programación. Este campo es necesario si la granularidad se establece en `monthly`.
  - <DAY_OF_WEEK>: *(Opcional)* El día de la semana (0 - 7) en el que se debe ejecutar la programación. Los valores de 0 o 7 indican el domingo. Este campo es necesario si la granularidad se establece en `weekly`.
  - <HOUR_OF_DAY>: *(Opcional)* La hora del día (0 - 23) que debe ejecutarse la programación. Este campo es necesario si la granularidad se establece en `daily`, `weekly`, o. `monthly`.
  - <MINUTE_OF_HOUR>: *(Opcional)* El minuto de la hora (0 - 59) que debe ejecutarse la programación. Este campo es necesario si la granularidad se establece en `hourly`, `daily`, `weekly`, o. `monthly`.

```
apiVersion: astra.netapp.io/v1
kind: Schedule
metadata:
  namespace: astra-connector
  name: <CR_NAME>
spec:
  applicationRef: <APPLICATION_NAME>
  appVaultRef: <APPVAULT_NAME>
  backupRetention: "<BACKUPS_RETAINED>"
  snapshotRetention: "<SNAPSHOTS_RETAINED>"
  granularity: <GRANULARITY>
  dayOfMonth: "<DAY_OF_MONTH>"
  dayOfWeek: "<DAY_OF_WEEK>"
  hour: "<HOUR_OF_DAY>"
  minute: "<MINUTE_OF_HOUR>"
```

2. Después de rellenar el `astra-control-schedule-cr.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -f astra-control-schedule-cr.yaml
```

Resultado

Astra Control implementa la política de protección de datos mediante la creación y retención de copias Snapshot y copias de seguridad con la política de programación y retención que haya definido.

Crear una copia de Snapshot

Puede crear una snapshot bajo demanda en cualquier momento.

Acerca de esta tarea

Astra Control permite la creación de copias Snapshot con clases de almacenamiento respaldadas por los siguientes controladores:

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

> Si su aplicación utiliza una clase de almacenamiento respaldada por `ontap-nas-economy` controlador, no se pueden crear instantáneas. Utilice una clase de almacenamiento alternativa para las instantáneas.

Cree una copia Snapshot de con la interfaz de usuario web de

Pasos

1. Seleccione **aplicaciones**.
2. En el menú Opciones de la columna **acciones** de la aplicación deseada, seleccione **Snapshot**.
3. Personalice el nombre de la instantánea y, a continuación, seleccione **Siguiente**.
4. [**Vista previa tecnológica**] Elija un cubo de destino para la instantánea de la lista de cubos de almacenamiento.
5. Revise el resumen de la instantánea y seleccione **Snapshot**.

[Vista previa técnica] Crear una instantánea con un CR

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre `astra-control-snapshot-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tu entorno de Astra Control y la configuración del clúster:
   - <CR_NAME>: El nombre de este recurso personalizado; elija un nombre único y sensible para su entorno.
   - <APPLICATION_NAME>: El nombre de Kubernetes de la aplicación que se va a realizar la instantánea.
   - <APPVAULT_NAME>: El nombre del AppVault donde se debe almacenar el contenido de la instantánea.
   - <RECLAIM_POLICY>: *(Opcional)* define lo que ocurre con una instantánea cuando se elimina la CR de instantánea. Opciones válidas:
     - `Retain`
     - `Delete` (predeterminado)

```
apiVersion: astra.netapp.io/v1
kind: Snapshot
metadata:
  namespace: astra-connector
  name: <CR_NAME>
spec:
  applicationRef: <APPLICATION_NAME>
  appVaultRef: <APPVAULT_NAME>
  reclaimPolicy: <RECLAIM_POLICY>
```

2. Después de rellenar el `astra-control-snapshot-cr.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -f astra-control-snapshot-cr.yaml
```

Resultado

Se inicia el proceso Snapshot. Una instantánea se realiza correctamente cuando el estado es **saludable** en la columna **Estado** de la página **Protección de datos** > **instantáneas**.

Cree un backup

También puede realizar copias de seguridad de una aplicación en cualquier momento.

> Sepa cómo se maneja el espacio de almacenamiento al realizar un backup de una aplicación alojada en el almacenamiento de Azure NetApp Files. Consulte "Backups de aplicaciones" si quiere más información.

> Astra Control permite la creación de backups mediante clases de almacenamiento respaldadas por los siguientes controladores:
>
> - `ontap-nas`
> - `ontap-nas-economy`
> - `ontap-san`
> - `ontap-san-economy`

Acerca de esta tarea

Los buckets en Astra Control no informan sobre la capacidad disponible. Antes de realizar backups o clonar aplicaciones gestionadas por Astra Control, comprueba la información del bucket en el sistema de administración del almacenamiento correspondiente.

Si su aplicación utiliza una clase de almacenamiento respaldada por `ontap-nas-economy` conductor, usted necesita habilite el backup y la restauración funcionalidad. Asegúrese de que ha definido un `backendType` parámetro en la "Objeto de almacenamiento de Kubernetes" con un valor de `ontap-nas-economy` antes de ejecutar cualquier operación de protección.

Cree un backup con la interfaz de usuario web de

Pasos

1. Seleccione **aplicaciones**.
2. En el menú Opciones de la columna **acciones** de la aplicación deseada, seleccione **copia de seguridad**.
3. Personalice el nombre del backup.
4. Elija si desea realizar una copia de seguridad de la aplicación desde una instantánea existente. Si selecciona esta opción, puede elegir entre una lista de snapshots existentes.
5. [**Tech preview**] Elija un depósito de destino para la copia de seguridad de la lista de depósitos de almacenamiento.
6. Seleccione **Siguiente**.
7. Revise el resumen de copia de seguridad y seleccione **copia de seguridad**.

[Vista previa técnica] Cree un backup con un CR

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre `astra-control-backup-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tu entorno de Astra Control y la configuración del clúster:
   - <CR_NAME>: El nombre de este recurso personalizado; elija un nombre único y sensible para su entorno.
   - <APPLICATION_NAME>: El nombre de Kubernetes de la aplicación de la que se va a realizar el backup.
   - <APPVAULT_NAME>: El nombre del AppVault donde se debe almacenar el contenido de la copia de seguridad.

   ```
   apiVersion: astra.netapp.io/v1
   kind: Backup
   metadata:
     namespace: astra-connector
     name: <CR_NAME>
   spec:
     applicationRef: <APPLICATION_NAME>
     appVaultRef: <APPVAULT_NAME>
   ```

2. Después de rellenar el `astra-control-backup-cr.yaml` Con los valores correctos, aplique el CR:

   ```
   kubectl apply -f astra-control-backup-cr.yaml
   ```

Resultado

Astra Control crea una copia de seguridad de la aplicación.

- Si la red tiene una interrupción del servicio o es anormalmente lenta, es posible que se agote el tiempo de espera de una operación de backup. Esto provoca un error en el backup.
- Si necesita cancelar una copia de seguridad en ejecución, utilice las instrucciones de Cancelar backups. Para eliminar la copia de seguridad, espere hasta que haya finalizado y, a continuación, utilice las instrucciones de Eliminar backups.
- Después de una operación de protección de datos (clonado, backup, restauración) y un cambio de tamaño posterior de volumen persistente, se demora hasta veinte minutos antes de que se muestre el tamaño del nuevo volumen en la interfaz de usuario. La operación de protección de datos se realiza correctamente en cuestión de minutos, y se puede utilizar el software de gestión para el back-end de almacenamiento para confirmar el cambio de tamaño del volumen.

Habilite el backup y la restauración para las operaciones económicas de ontap-nas

Astra Control Provisioning ofrece funcionalidad de backup y restauración que puede habilitarse para los back-ends de almacenamiento que utilicen el `ontap-nas-economy` clase de almacenamiento.

Antes de empezar

- Habilitó el aprovisionador de Astra Control o Astra Trident.
- Has definido una aplicación en Astra Control. Esta aplicación tendrá funcionalidad de protección limitada hasta que complete este procedimiento.
- Ya tienes `ontap-nas-economy` se ha seleccionado como la clase de almacenamiento predeterminada para el back-end del almacenamiento.

Expanda para obtener pasos de configuración

1. Realice lo siguiente en el back-end de almacenamiento de ONTAP:

   a. Busque la SVM donde aloja el `ontap-nas-economy`-basado en volúmenes de la aplicación.

   b. Inicie sesión en un terminal conectado a ONTAP donde se crean los volúmenes.

   c. Oculte el directorio de snapshots para la SVM:

   > Este cambio afecta a toda la SVM. El directorio oculto seguirá siendo accesible.

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

+

> Compruebe que el directorio de snapshots del back-end de almacenamiento de ONTAP esté oculto. Si no se oculta este directorio, se puede perder el acceso a la aplicación, especialmente si se utiliza NFSv3.

2. Haga lo siguiente en Astra Control Provisioner o Astra Trident:

   a. Habilite el directorio snapshot para cada VP basado en ontap-nas y asociado con la aplicación:

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

   b. Confirme que el directorio de snapshots se haya habilitado para cada VP asociado:

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

   Respuesta:

```
snapshotDirectory: "true"
```

3. En Astra Control, actualiza la aplicación después de habilitar todos los directorios Snapshot asociados para que Astra Control reconozca el valor modificado.

Resultado

La aplicación está lista para realizar backups y restauraciones con Astra Control. Otras aplicaciones también pueden utilizar cada RVP para realizar backups y restauraciones de datos.

Cree un backup inmutable

No se puede modificar, eliminar ni sobrescribir una copia de seguridad inmutable siempre que la política de retención del depósito que almacena la copia de seguridad la prohíba. Puede crear backups inmutables mediante el backup de aplicaciones en bloques que tengan configurada una política de retención. Consulte "Protección de datos" para obtener información importante sobre cómo trabajar con backups inmutables.

Antes de empezar

Debe configurar el bucket de destino con una política de retención. La forma de hacerlo variará en función del proveedor de almacenamiento que utilice. Consulte la documentación del proveedor de almacenamiento para obtener más información:

- **Amazon Web Services**: "Habilite S3 Object Lock al crear el bloque y establezca un modo de retención predeterminado de «gobierno» con un período de retención predeterminado".
- **Google Cloud**: "Configure un depósito con una política de retención y especifique un período de retención".
- **Microsoft Azure**: "Configure un depósito de almacenamiento BLOB con una política de retención basada en tiempo en el ámbito de nivel de contenedor".
- **NetApp StorageGRID**: "Habilite S3 Object Lock al crear el bloque y establezca un modo de retención predeterminado de «cumplimiento» con un período de retención predeterminado".

> Los buckets en Astra Control no informan sobre la capacidad disponible. Antes de realizar backups o clonar aplicaciones gestionadas por Astra Control, comprueba la información del bucket en el sistema de administración del almacenamiento correspondiente.

> Si su aplicación utiliza una clase de almacenamiento respaldada por `ontap-nas-economy` controlador, asegúrese de que ha definido un `backendType` parámetro en la "Objeto de almacenamiento de Kubernetes" con un valor de `ontap-nas-economy` antes de ejecutar cualquier operación de protección.

Pasos

1. Seleccione **aplicaciones**.
2. En el menú Opciones de la columna **acciones** de la aplicación deseada, seleccione **copia de seguridad**.
3. Personalice el nombre del backup.
4. Elija si desea realizar una copia de seguridad de la aplicación desde una instantánea existente. Si selecciona esta opción, puede elegir entre una lista de snapshots existentes.
5. Seleccione un bucket de destino para el backup en la lista de bloques de almacenamiento. Se indica un depósito de escritura única y lectura múltiple (WORM) con el estado «bloqueado» junto al nombre del depósito.

   > Si el depósito es de tipo no admitido, se indica cuando pasa el ratón por encima o selecciona el depósito.

6. Seleccione **Siguiente**.
7. Revise el resumen de copia de seguridad y seleccione **copia de seguridad**.

Resultado

Astra Control crea un backup inmutable de la aplicación.

- Si la red tiene una interrupción del servicio o es anormalmente lenta, es posible que se agote el tiempo de espera de una operación de backup. Esto provoca un error en el backup.
- Si intentas crear dos backups inmutables de la misma aplicación en el mismo bloque a la vez, Astra Control impide que se inicie el segundo backup. Espere hasta que se complete la primera copia de seguridad antes de iniciar otra.
- No es posible cancelar una copia de seguridad inmutable en ejecución.
- Después de una operación de protección de datos (clonado, backup, restauración) y un cambio de tamaño posterior de volumen persistente, se demora hasta veinte minutos antes de que se muestre el tamaño del nuevo volumen en la interfaz de usuario. La operación de protección de datos se realiza correctamente en cuestión de minutos, y se puede utilizar el software de gestión para el back-end de almacenamiento para confirmar el cambio de tamaño del volumen.

Ver Snapshot y backups

Puede ver las instantáneas y las copias de seguridad de una aplicación desde la pestaña Data Protection.

Se indica una copia de seguridad inmutable con el estado «Locked» junto al bloque que está utilizando.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
2. Seleccione **Protección de datos**.

   Las instantáneas se muestran de forma predeterminada.

3. Seleccione **copias de seguridad** para consultar la lista de copias de seguridad.

Eliminar snapshots

Elimine las snapshots programadas o bajo demanda que ya no necesite.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
2. Seleccione **Protección de datos**.
3. En el menú Opciones de la columna **acciones** de la instantánea deseada, seleccione **Eliminar instantánea**.
4. Escriba la palabra "delete" para confirmar la eliminación y, a continuación, seleccione **Yes, Delete snapshot**.

Resultado

Astra Control elimina la instantánea.

Cancelar backups

Es posible cancelar una copia de seguridad que esté en curso.

Para cancelar una copia de seguridad, la copia de seguridad debe estar en `Running` estado. No puede cancelar una copia de seguridad que esté en `Pending` estado.

No es posible cancelar una copia de seguridad inmutable en ejecución.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. Seleccione **Protección de datos**.
3. Seleccione **copias de seguridad**.
4. En el menú Opciones de la columna **acciones** para la copia de seguridad deseada, seleccione **Cancelar**.
5. Escriba la palabra "cancelar" para confirmar la operación y, a continuación, seleccione **Sí, cancelar copia de seguridad**.

Eliminar backups

Elimine los backups programados o bajo demanda que ya no necesita.

Si necesita cancelar una copia de seguridad en ejecución, utilice las instrucciones de Cancelar backups. Para eliminar la copia de seguridad, espere hasta que haya finalizado y, a continuación, utilice estas instrucciones.

No se puede eliminar un backup inmutable antes de que caduque el período de retención.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. Seleccione **Protección de datos**.
3. Seleccione **copias de seguridad**.
4. En el menú Opciones de la columna **acciones** de la copia de seguridad deseada, seleccione **Eliminar copia de seguridad**.
5. Escriba la palabra "delete" para confirmar la eliminación y, a continuación, seleccione **Yes, Delete backup**.

Resultado

Astra Control elimina la copia de seguridad.

[Tech preview] Proteger todo un clúster

Es posible crear un backup automático programado de cualquiera de los espacios de nombres no gestionados de un clúster o de todos ellos. Estos flujos de trabajo los proporciona NetApp como una cuenta de servicio de Kubernetes, enlaces de roles y un trabajo cron orquestado con un script de Python.

Cómo funciona

Cuando configura e instala el flujo de trabajo de backup de clúster completo, un trabajo con cron se ejecuta periódicamente y protege cualquier espacio de nombres que aún no esté gestionado, lo que crea automáticamente políticas de protección basadas en los programas que elija durante la instalación.

Si no desea proteger todos los espacios de nombres no administrados en el clúster con el flujo de trabajo de backup de clúster completo, en su lugar, puede utilizar el flujo de trabajo de backup basado en etiquetas. El flujo de trabajo de backup basado en etiquetas también usa una tarea CRON, pero, en lugar de proteger todos

los espacios de nombres no gestionados, identifica los espacios de nombres por etiquetas que se proporcionan para proteger, opcionalmente, los espacios de nombres según políticas de backup bronce, plata o oro.

Cuando se crea un nuevo espacio de nombres que se ajusta al alcance del flujo de trabajo elegido, se protege automáticamente, sin necesidad de que el administrador realice ninguna acción. Estos flujos de trabajo se implementan por clúster, de modo que diferentes clústeres pueden utilizar cualquier flujo de trabajo con niveles de protección únicos, según la importancia del clúster.

Ejemplo: Protección de clúster completa

Como ejemplo, cuando configura e instala el flujo de trabajo de backup completo del clúster, las aplicaciones en cualquier espacio de nombres se gestionan periódicamente y se protegen sin que el administrador intervenga. El espacio de nombres no tiene que existir en el momento de instalar el flujo de trabajo; si se agrega un espacio de nombres en el futuro, se protegerá.

Ejemplo: Protección basada en etiquetas

Para obtener más granularidad, puede utilizar el flujo de trabajo basado en etiquetas. Por ejemplo, puede instalar este flujo de trabajo y decirle a los usuarios que apliquen una de varias etiquetas a cualquier espacio de nombres que quieran proteger, según el nivel de protección que necesiten. Esto permite a los usuarios crear el espacio de nombres con una de estas etiquetas, y no tienen que notificar a un administrador. Su nuevo espacio de nombres y todas las aplicaciones que contiene quedan protegidas de forma automática.

Cree una copia de seguridad programada de todos los espacios de nombres

Es posible crear un backup programado de todos los espacios de nombres en un clúster mediante el flujo de trabajo de backup de clúster completo.

Pasos

1. Descargue los siguientes archivos en una máquina que tenga acceso a la red al clúster:
   - "Archivo CRD Components.yaml"
   - "protectCluster.py Script Python"
2. Para configurar e instalar el kit de herramientas: "siga las instrucciones incluidas".

Crear una copia de seguridad programada de espacios de nombres específicos

Puede crear un backup programado de espacios de nombres específicos mediante sus etiquetas mediante el flujo de trabajo de backup basado en etiquetas.

Pasos

1. Descargue los siguientes archivos en una máquina que tenga acceso a la red al clúster:
   - "Archivo CRD Components.yaml"
   - "protectCluster.py Script Python"
2. Para configurar e instalar el kit de herramientas: "siga las instrucciones incluidas".

Restaurar aplicaciones

Astra Control puede restaurar su aplicación a partir de una instantánea o una copia de seguridad. La restauración a partir de una snapshot existente será más rápida cuando se restaure la aplicación en el mismo clúster. Puede utilizar la interfaz de usuario de Astra Control o. "La API de control Astra" para restaurar aplicaciones.

> Si se agrega un filtro de espacio de nombres a un enlace de ejecución que se ejecuta después de una operación de restauración o clonado y el origen y destino de la restauración o clonado se encuentran en diferentes espacios de nombres, el filtro de espacio de nombres solo se aplica al espacio de nombres de destino.

Antes de empezar

- **Proteja sus aplicaciones primero**: Se recomienda encarecidamente que tome una instantánea o una copia de seguridad de su aplicación antes de restaurarla. Esto le permitirá clonar desde la snapshot o backup si la restauración no se realiza correctamente.
- **Comprobar volúmenes de destino**: Si restaura a una clase de almacenamiento diferente, asegúrese de que la clase de almacenamiento utilice el mismo modo de acceso de volumen persistente (por ejemplo, ReadWriteMany). Se producirá un error en la operación de restauración si el modo de acceso al volumen persistente de destino es diferente. Por ejemplo, si el volumen persistente de origen utiliza el modo de acceso RWX, seleccionando una clase de almacenamiento de destino que no pueda proporcionar RWX, como Azure Managed Disks, AWS EBS, Google Persistent Disk o. `ontap-san`, hará que falle la operación de restauración. Para obtener más información sobre los modos de acceso a volúmenes persistentes, consulte la "Kubernetes" documentación.
- **Planificar necesidades de espacio**: Cuando se realiza una restauración in situ de una aplicación que utiliza almacenamiento ONTAP de NetApp, el espacio utilizado por la aplicación restaurada puede duplicarse. Después de realizar una restauración sin movimiento, elimine las instantáneas no deseadas de la aplicación restaurada para liberar espacio de almacenamiento.
- **Controladores de clase de almacenamiento compatibles**: Astra Control admite la restauración de copias de seguridad mediante clases de almacenamiento respaldadas por los siguientes controladores:
  - `ontap-nas`
  - `ontap-nas-economy`
  - `ontap-san`
  - `ontap-san-economy`
- **(Solo controlador económico de ontap-nas) Copias de seguridad y restauraciones**: Antes de realizar copias de seguridad o restaurar una aplicación que utiliza una clase de almacenamiento respaldada por el `ontap-nas-economy` controlador, compruebe que el "El directorio Snapshot del sistema de administración de almacenamiento de ONTAP está oculto". Si no se oculta este directorio, se puede perder el acceso a la aplicación, especialmente si se utiliza NFSv3.

> La ejecución de una operación de restauración sin movimiento en una aplicación que comparte recursos con otra aplicación puede tener resultados no intencionados. Los recursos compartidos entre las aplicaciones se reemplazan cuando se realiza una restauración sin movimiento en una de las aplicaciones.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. En el menú Opciones de la columna Acciones, seleccione **Restaurar**.
3. Elija el tipo de restauración:
   - **Restaurar en espacios de nombres originales**: Utilice este procedimiento para restaurar la aplicación en su sitio al cluster original.
     i. Seleccione la instantánea o la copia de seguridad que desea utilizar para restaurar la aplicación en el lugar, lo que revierte la aplicación a una versión anterior de sí misma.

ii. Seleccione **Siguiente**.

> Si se restaura en un espacio de nombres que se eliminó previamente, se crea un espacio de nombres nuevo con el mismo nombre como parte del proceso de restauración. Cualquier usuario que tenga derechos para administrar aplicaciones en el espacio de nombres previamente eliminado debe restaurar manualmente los derechos en el espacio de nombres recién creado.

- **Restaurar en nuevos espacios de nombres**: Utilice este procedimiento para restaurar la aplicación en otro clúster o con diferentes espacios de nombres desde el origen. También puede usar este procedimiento para migrar una aplicación a una clase de almacenamiento diferente.
  i. Especifique el nombre de la aplicación restaurada.
  ii. Elija el clúster de destino de la aplicación que desea restaurar.
  iii. Introduzca un espacio de nombres de destino para cada espacio de nombres de origen asociado a la aplicación.

  > Astra Control crea nuevos espacios de nombres de destino como parte de esta opción de restauración. Los espacios de nombres de destino que especifique no deben estar ya presentes en el clúster de destino.

  iv. Seleccione **Siguiente**.
  v. Seleccione la instantánea o la copia de seguridad que desea utilizar para restaurar la aplicación.
  vi. Seleccione **Siguiente**.
  vii. Elija una de las siguientes opciones:
    - **Restaurar usando clases de almacenamiento originales**: La aplicación utiliza la clase de almacenamiento asociada originalmente a menos que no exista en el clúster de destino. En este caso, se utilizará la clase de almacenamiento predeterminada para el clúster.
    - **Restaurar usando una clase de almacenamiento diferente**: Seleccione una clase de almacenamiento que exista en el clúster de destino. Todos los volúmenes de aplicaciones, independientemente de sus tipos de almacenamiento asociados originalmente, se migrarán a esta clase de almacenamiento diferente como parte de la restauración.
  viii. Seleccione **Siguiente**.

4. Elija cualquier recurso para filtrar:
   - **Restaurar todos los recursos**: Restaurar todos los recursos asociados con la aplicación original.
   - **Filtrar recursos**: Especificar reglas para restaurar un subconjunto de los recursos originales de la aplicación:
     i. Seleccione incluir o excluir recursos de la aplicación restaurada.
     ii. Seleccione **Agregar regla de inclusión** o **Agregar regla de exclusión** y configure la regla para filtrar los recursos correctos durante la restauración de la aplicación. Puede editar una regla o eliminarla y volver a crear una regla hasta que la configuración sea correcta.

     > Para obtener más información sobre la configuración de reglas de inclusión y exclusión, consulte Filtre recursos durante una restauración de aplicación.

5. Seleccione **Siguiente**.
6. Revise los detalles sobre la acción de restauración cuidadosamente, escriba “restaurar” (si se le solicita) y

seleccione **Restaurar**.

[Vista previa técnica] Restaurar a partir del backup mediante un recurso personalizado (CR)

Es posible restaurar datos desde un backup con un archivo de recurso personalizado (CR) en otro espacio de nombres o en el espacio de nombres de origen original.

Restaurar desde una copia de seguridad con un CR

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre `astra-control-backup-restore-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tu entorno de Astra Control y la configuración del clúster:
   - <CR_NAME>: El nombre de esta operación de CR; seleccione un nombre sensible para su entorno.
   - <APPVAULT_NAME>: El nombre del AppVault donde se almacena el contenido del backup.
   - <BACKUP_PATH>: Ruta dentro de AppVault, donde se almacena el contenido del backup. Por ejemplo:

     ```
     ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
     20231213023800_94347756-9d9b-401d-a0c3
     ```

   - <SOURCE_NAMESPACE>: El espacio de nombres de origen de la operación de restauración.
   - <DESTINATION_NAMESPACE>: El espacio de nombres de destino de la operación de restauración.

     ```
     apiVersion: astra.netapp.io/v1
     kind: BackupRestore
     metadata:
       name: <CR_NAME>
       namespace: astra-connector
     spec:
       appVaultRef: <APPVAULT_NAME>
       appArchivePath: <BACKUP_PATH>
       namespaceMapping: [{"source": "<SOURCE_NAMESPACE>",
     "destination": "<DESTINATION_NAMESPACE>"}]
     ```

Directiva no resuelta en <stdin> - Include:../_include/selective-restore-cr.adoc[]

1. Después de rellenar el `astra-control-backup-restore-cr.yaml` Con los valores correctos, aplique el CR:

   ```
   kubectl apply -f astra-control-backup-restore-cr.yaml
   ```

Restaure desde un backup al espacio de nombres original con un CR

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre `astra-control-backup-ipr-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tu entorno de Astra Control y la configuración del clúster:
   - <CR_NAME>: El nombre de esta operación de CR; seleccione un nombre sensible para su

entorno.

- <APPVAULT_NAME>: El nombre del AppVault donde se almacena el contenido del backup.
- <BACKUP_PATH>: Ruta dentro de AppVault, donde se almacena el contenido del backup. Por ejemplo:

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
20231213023800_94347756-9d9b-401d-a0c3
```

```yaml
apiVersion: astra.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appVaultRef: <APPVAULT_NAME>
  appArchivePath: <BACKUP_PATH>
```

Directiva no resuelta en <stdin> - Include:../_include/selective-restore-cr.adoc[]

1. Después de rellenar el `astra-control-backup-ipr-cr.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -f astra-control-backup-ipr-cr.yaml
```

[Vista PREVIA TÉCNICA] Restauración a partir de una instantánea con un recurso personalizado (CR)

Puede restaurar datos desde una copia Snapshot con un archivo de recurso personalizado (CR) en un espacio de nombres diferente o en el espacio de nombres de origen original.

Restaurar desde instantánea con un CR

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre `astra-control-snapshot-restore-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tu entorno de Astra Control y la configuración del clúster:
   - <CR_NAME>: El nombre de esta operación de CR; seleccione un nombre sensible para su entorno.
   - <APPVAULT_NAME>: El nombre del AppVault donde se almacena el contenido del backup.
   - <BACKUP_PATH>: Ruta dentro de AppVault, donde se almacena el contenido del backup. Por ejemplo:

     ```
     ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
     20231213023800_94347756-9d9b-401d-a0c3
     ```

   - <SOURCE_NAMESPACE>: El espacio de nombres de origen de la operación de restauración.
   - <DESTINATION_NAMESPACE>: El espacio de nombres de destino de la operación de restauración.

     ```
     apiVersion: astra.netapp.io/v1
     kind: SnapshotRestore
     metadata:
       name: <CR_NAME>
       namespace: astra-connector
     spec:
       appArchivePath: <BACKUP_PATH>
       appVaultRef: <APPVAULT_NAME>
       namespaceMapping: [{"source": "<SOURCE_NAMESPACE>",
     "destination": "<DESTINATION_NAMESPACE>"}]
     ```

Directiva no resuelta en <stdin> - Include:../_include/selective-restore-cr.adoc[]

1. Después de rellenar el `astra-control-snapshot-restore-cr.yaml` Con los valores correctos, aplique el CR:

   ```
   kubectl apply -f astra-control-snapshot-restore-cr.yaml
   ```

Restauración de una snapshot al espacio de nombres original con un CR

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre `astra-control-snapshot-ipr-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tu entorno de Astra Control y la configuración del clúster:
   - <CR_NAME>: El nombre de esta operación de CR; seleccione un nombre sensible para su

entorno.

- <APPVAULT_NAME>: El nombre del AppVault donde se almacena el contenido del backup.
- <BACKUP_PATH>: Ruta dentro de AppVault, donde se almacena el contenido del backup. Por ejemplo:

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
20231213023800_94347756-9d9b-401d-a0c3
```

```yaml
apiVersion: astra.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appArchivePath: <BACKUP_PATH>
  appVaultRef: <APPVAULT_NAME>
```

Directiva no resuelta en <stdin> - Include:../_include/selective-restore-cr.adoc[]

1. Después de rellenar el `astra-control-snapshot-ipr-cr.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -f astra-control-snapshot-ipr-cr.yaml
```

Resultado

Astra Control restaura la aplicación en función de la información proporcionada. Si restauró la aplicación en un lugar, el contenido de los volúmenes persistentes existentes se reemplaza por el contenido de los volúmenes persistentes de la aplicación restaurada.

> Después de una operación de protección de datos (clonado, backup o restauración) y un posterior tamaño de volumen persistente, se produce un retraso de hasta veinte minutos antes de que se muestre el tamaño del nuevo volumen en la interfaz de usuario web. La operación de protección de datos se realiza correctamente en cuestión de minutos, y se puede utilizar el software de gestión para el back-end de almacenamiento para confirmar el cambio de tamaño del volumen.

> Cualquier usuario miembro con restricciones de espacio de nombres por nombre/ID de espacio de nombres o por etiquetas de espacio de nombres puede clonar o restaurar una aplicación en un nuevo espacio de nombres en el mismo clúster o en cualquier otro clúster de la cuenta de su organización. Sin embargo, el mismo usuario no puede acceder a la aplicación clonada o restaurada en el nuevo espacio de nombres. Después de que una operación de clonado o restauración crea un nuevo espacio de nombres, el administrador/propietario de la cuenta puede editar la cuenta de usuario miembro y actualizar las restricciones de roles para el usuario afectado a fin de otorgar acceso al nuevo espacio de nombres.

Filtre recursos durante una restauración de aplicación

Puede agregar una regla de filtro a un "restaurar" operación que especificará los recursos de aplicación existentes que se incluirán o excluirán de la aplicación restaurada. Puede incluir o excluir recursos basados en un espacio de nombres, etiqueta o GVK (GroupVersionKind) especificado.

Lea más sobre Incluir y excluir escenarios

- **Selecciona una regla de inclusión con espacios de nombres originales (restauración in situ)**: Los recursos de aplicación existentes que definas en la regla se eliminarán y reemplazarán por aquellos de la instantánea o copia de seguridad seleccionada que estés utilizando para la restauración. Cualquier recurso que no especifique en la regla Incluir permanecerá sin cambios.
- **Selecciona una regla de inclusión con nuevos espacios de nombres**: Usa la regla para seleccionar los recursos específicos que deseas en la aplicación restaurada. Los recursos que no especifique en la regla Incluir no se incluirán en la aplicación restaurada.
- **Selecciona una regla de exclusión con espacios de nombres originales (restauración in situ)**: Los recursos que especifiques para ser excluidos no se restaurarán y permanecerán sin cambios. Los recursos que no especifique para excluir se restaurarán de la Snapshot o el backup. Todos los datos de los volúmenes persistentes se eliminarán y volverán a crear si el StatefulSet correspondiente forma parte de los recursos filtrados.
- **Selecciona una regla de exclusión con nuevos espacios de nombres**: Usa la regla para seleccionar los recursos específicos que deseas eliminar de la aplicación restaurada. Los recursos que no especifique para excluir se restaurarán de la Snapshot o el backup.

Las reglas son tipos de inclusión o exclusión. Las reglas que combinan la inclusión y exclusión de recursos no están disponibles.

Pasos

1. Una vez que haya elegido filtrar recursos y seleccionado una opción Incluir o Excluir en el asistente Restaurar aplicación, seleccione **Agregar regla de inclusión** o **Agregar regla de exclusión**.

   No puede excluir ningún recurso en el ámbito del clúster que Astra Control incluya automáticamente.

2. Configure la regla de filtro:

   Debe especificar al menos un espacio de nombres, una etiqueta o un GVK. Asegúrese de que los recursos que retenga después de aplicar las reglas de filtro sean suficientes para mantener la aplicación restaurada en buen estado.

   a. Seleccione un espacio de nombres específico para la regla. Si no hace una selección, se usarán todos los espacios de nombres en el filtro.

      Si la aplicación contenía originalmente varios espacios de nombres y la restauraba en nuevos espacios de nombres, todos los espacios de nombres se crearán incluso si no contienen recursos.

   b. (Opcional) Introduzca un nombre de recurso.

   c. (Opcional) **Selector de etiquetas**: Incluye a. "selector de etiquetas" para agregar a la regla. El selector de etiquetas se utiliza para filtrar sólo los recursos que coincidan con la etiqueta seleccionada.

d. (Opcional) Seleccione **Usar GVK (GroupVersionKind) configurado para filtrar recursos** para opciones de filtrado adicionales.

> Si utiliza un filtro GVK, debe especificar Versión y Tipo.

i. (Opcional) **Grupo**: En la lista desplegable, seleccione el grupo API de Kubernetes.

ii. **Kind**: En la lista desplegable, seleccione el esquema de objeto para el tipo de recurso de Kubernetes a utilizar en el filtro.

iii. **Versión**: Seleccione la versión de la API de Kubernetes.

3. Revise la regla que se crea en función de las entradas.
4. Seleccione **Agregar**.

> Puede crear tantas reglas de inclusión y exclusión de recursos como desee. Las reglas aparecen en el resumen de la aplicación de restauración antes de iniciar la operación.

Clone y migre aplicaciones

Puede clonar una aplicación existente para crear una aplicación duplicada en el mismo clúster de Kubernetes o en otro clúster. Cuando Astra Control clona una aplicación, crea un clon de la configuración de la aplicación y del almacenamiento persistente.

El clonado puede ayudarle si necesita mover aplicaciones y almacenamiento de un clúster de Kubernetes a otro. Por ejemplo, es posible que desee mover cargas de trabajo mediante una canalización de CI/CD y entre espacios de nombres Kubernetes.

> Si se agrega un filtro de espacio de nombres a un enlace de ejecución que se ejecuta después de una operación de restauración o clonado y el origen y destino de la restauración o clonado se encuentran en diferentes espacios de nombres, el filtro de espacio de nombres solo se aplica al espacio de nombres de destino.

Antes de empezar

- **Comprobar volúmenes de destino**: Si clona a una clase de almacenamiento diferente, asegúrese de que la clase de almacenamiento utilice el mismo modo de acceso de volumen persistente (por ejemplo, ReadWriteMany). Se producirá un error en la operación de clonado si el modo de acceso al volumen persistente de destino es diferente. Por ejemplo, si el volumen persistente de origen utiliza el modo de acceso RWX, seleccionando una clase de almacenamiento de destino que no pueda proporcionar RWX, como Azure Managed Disks, AWS EBS, Google Persistent Disk o. `ontap-san`, hará que se produzca un error en la operación de clonado. Para obtener más información sobre los modos de acceso a volúmenes persistentes, consulte la "Kubernetes" documentación.
- Para clonar aplicaciones en un clúster diferente, debe asegurarse de haber asignado un bloque predeterminado para la instancia de cloud que contiene el clúster de origen. Si la instancia de cloud de origen no tiene un conjunto de bloques predeterminado, se producirá un error en la operación de clonado entre clústeres.
- Durante las operaciones de clonado, las aplicaciones que necesitan un recurso IngressClass o enlaces web para funcionar correctamente no deben tener esos recursos ya definidos en el clúster de destino.

Limitaciones de clones

- **Clases de almacenamiento explícitas**: Si implementa una aplicación con una clase de almacenamiento

definida explícitamente y necesita clonar la aplicación, el clúster de destino debe tener la clase de almacenamiento especificada originalmente. Se producirá un error al clonar una aplicación con una clase de almacenamiento definida explícitamente a un clúster que no tenga la misma clase de almacenamiento.

- **Aplicaciones respaldadas por la economía de ontap-nas**: No puede usar operaciones de clonación si la clase de almacenamiento de su aplicación está respaldada por el `ontap-nas-economy` controlador. Sin embargo, usted puede "habilite el backup y la restauración para las operaciones económicas de ontap-nas".
- **Clones y restricciones de usuario**: Cualquier usuario miembro con restricciones de espacio de nombres por nombre/ID de espacio de nombres o por etiquetas de espacio de nombres puede clonar o restaurar una aplicación a un nuevo espacio de nombres en el mismo clúster o a cualquier otro clúster de la cuenta de su organización. Sin embargo, el mismo usuario no puede acceder a la aplicación clonada o restaurada en el nuevo espacio de nombres. Después de que una operación de clonado o restauración crea un nuevo espacio de nombres, el administrador/propietario de la cuenta puede editar la cuenta de usuario miembro y actualizar las restricciones de roles para el usuario afectado a fin de otorgar acceso al nuevo espacio de nombres.
- **Los clones utilizan cubos predeterminados**:
  - Durante una copia de seguridad de la aplicación o una restauración de la aplicación, puede especificar un bloque que se va a utilizar. Debe especificar un bloque predeterminado cuando se clona en clústeres, pero especificar un bloque es opcional cuando se clona dentro del mismo clúster.
  - Cuando se clona en un clúster, la instancia de cloud que contiene el clúster de origen de la operación de clonado debe tener un conjunto de bloques predeterminado.
  - No existe ninguna opción para cambiar bloques para un clon. Si desea controlar qué segmento se utiliza, puede hacer lo mismo "cambiar el valor predeterminado del segmento" o haga un "Backup" seguido de un "restaurar" por separado.
- **Con Jenkins CI**: Si clona una instancia de Jenkins CI desplegada por el operador, debe restaurar manualmente los datos persistentes. Esta es una limitación del modelo de puesta en marcha de la aplicación.

Pasos

1. Seleccione **aplicaciones**.
2. Debe realizar una de las siguientes acciones:
   - Seleccione el menú Opciones de la columna **acciones** de la aplicación deseada.
   - Seleccione el nombre de la aplicación deseada y seleccione la lista desplegable de estado en la parte superior derecha de la página.
3. Seleccione **Clonar**.
4. Especifique los detalles del clon:
   - Introduzca un nombre.
   - Elija un clúster de destino para el clon.
   - Introduzca los espacios de nombres de destino para el clon. Cada espacio de nombres de origen asociado a la aplicación se asigna a un espacio de nombres de destino.

     > Astra Control crea nuevos espacios de nombres de destino como parte de la operación de clonación. Los espacios de nombres de destino que especifique no deben estar ya presentes en el clúster de destino.

   - Seleccione **Siguiente**.

- Elija mantener la clase de almacenamiento original asociada a la aplicación o seleccionar una clase de almacenamiento diferente.

> Puedes migrar una clase de almacenamiento de una aplicación a una clase de almacenamiento de proveedor de nube nativo u otro tipo de almacenamiento compatible, y migrar una aplicación desde una clase de almacenamiento respaldada por `ontap-nas-economy` a una clase de almacenamiento respaldada por `ontap-nas` en el mismo clúster o copie la aplicación en otro clúster con una clase de almacenamiento respaldada por `ontap-nas-economy` controlador.

> Si selecciona otra clase de almacenamiento y esta clase de almacenamiento no existe en el momento de la restauración, se devolverá un error.

5. Seleccione **Siguiente**.
6. Revise la información sobre el clon y seleccione **Clonar**.

Resultado

Astra Control clona la aplicación en función de la información proporcionada. La operación de clonado se realiza correctamente cuando se encuentra el nuevo clon de la aplicación `Healthy` en la página **aplicaciones**.

Después de que una operación de clonado o restauración crea un nuevo espacio de nombres, el administrador/propietario de la cuenta puede editar la cuenta de usuario miembro y actualizar las restricciones de roles para el usuario afectado a fin de otorgar acceso al nuevo espacio de nombres.

Gestione los enlaces de ejecución de aplicaciones

Un enlace de ejecución es una acción personalizada que puede configurar para que se ejecute junto con una operación de protección de datos de una aplicación gestionada. Por ejemplo, si dispone de una aplicación de base de datos, puede utilizar un enlace de ejecución para pausar todas las transacciones de la base de datos antes de realizar una instantánea y reanudar las transacciones una vez completada la instantánea. De este modo se garantiza la creación de instantáneas coherentes con la aplicación.

Tipos de enlaces de ejecución

Astra Control Service admite los siguientes tipos de ganchos de ejecución, según cuándo se puedan ejecutar:

- Copia previa de Snapshot
- Possnapshot
- Previo al backup
- Después del backup
- Después de la restauración

Filtros de gancho de ejecución

Al agregar o editar un enlace de ejecución a una aplicación, puede agregar filtros a un enlace de ejecución para gestionar los contenedores que coincidirá el enlace. Los filtros son útiles para aplicaciones que usan la misma imagen de contenedor en todos los contenedores, pero pueden usar cada imagen para un propósito

diferente (como Elasticsearch). Los filtros le permiten crear escenarios donde los enlaces de ejecución se ejecutan en algunos, pero no necesariamente todos los contenedores idénticos. Si crea varios filtros para un único enlace de ejecución, se combinan con un operador y lógico. Puede tener hasta 10 filtros activos por gancho de ejecución.

Cada filtro que agregue a un enlace de ejecución utiliza una expresión regular para hacer coincidir los contenedores del clúster. Cuando un gancho coincide con un contenedor, el gancho ejecutará su script asociado en ese contenedor. Las expresiones regulares para los filtros utilizan la sintaxis expresión regular 2 (RE2), que no admite la creación de un filtro que excluye contenedores de la lista de coincidencias. Para obtener información sobre la sintaxis que admite Astra Control para las expresiones regulares en los filtros de enlace de ejecución, consulte "Soporte de sintaxis de expresión regular 2 (RE2)".

> Si se agrega un filtro de espacio de nombres a un enlace de ejecución que se ejecuta después de una operación de restauración o clonado y el origen y destino de la restauración o clonado se encuentran en diferentes espacios de nombres, el filtro de espacio de nombres solo se aplica al espacio de nombres de destino.

Notas importantes sobre los enlaces de ejecución personalizados

Tenga en cuenta lo siguiente al planificar enlaces de ejecución para sus aplicaciones.

> Debido a que los enlaces de ejecución a menudo reducen o desactivan por completo la funcionalidad de la aplicación con la que se ejecutan, siempre debe intentar minimizar el tiempo que tardan los enlaces de ejecución personalizados.
> Si inicia una operación de copia de seguridad o de instantánea con los enlaces de ejecución asociados pero, a continuación, la cancela, los ganchos pueden ejecutarse si ya se ha iniciado la operación de copia de seguridad o de Snapshot. Esto significa que la lógica utilizada en un enlace de ejecución posterior a la copia de seguridad no puede suponer que la copia de seguridad se ha completado.

- La función de enlaces de ejecución está deshabilitada de forma predeterminada para las nuevas implementaciones de Astra Control.
  - Debe activar la función de enlaces de ejecución antes de poder utilizar los enlaces de ejecución.
  - Los usuarios propietario o administrador pueden habilitar o deshabilitar la función de enlaces de ejecución para todos los usuarios definidos en la cuenta de Astra Control actual. Consulte Active la función de enlaces de ejecución y.. Desactive la función de enlaces de ejecución si desea obtener instrucciones.
  - El estado de habilitación de la función se preserva durante las actualizaciones de Astra Control.
- Un enlace de ejecución debe utilizar una secuencia de comandos para realizar acciones. Muchos enlaces de ejecución pueden hacer referencia al mismo script.
- Astra Control requiere que las secuencias de comandos que utilizan los enlaces de ejecución se escriban en el formato de secuencias de comandos de shell ejecutables.
- El tamaño del script está limitado a 96 KB.
- Astra Control utiliza la configuración del enlace de ejecución y cualquier criterio coincidente para determinar qué ganchos se aplican a una operación de instantánea, copia de seguridad o restauración.
- Todos los fallos del enlace de ejecución son fallos de software; otros ganchos y la operación de protección de datos se siguen intentando incluso si falla un gancho. Sin embargo, cuando falla un gancho, se registra un suceso de advertencia en el registro de eventos de la página **Activity**.
- Para crear, editar o eliminar enlaces de ejecución, debe ser un usuario con permisos de propietario,

administrador o miembro.

- Si un enlace de ejecución tarda más de 25 minutos en ejecutarse, el enlace fallará, creando una entrada de registro de eventos con un código de retorno de "N/A". Se agotará el tiempo de espera de todas las instantáneas afectadas y se marcarán como errores, con una entrada de registro de eventos resultante que tenga en cuenta el tiempo de espera.
- Para las operaciones de protección de datos ad hoc, todos los eventos de enlace se generan y guardan en el registro de eventos de la página **Actividad**. Sin embargo, en el caso de las operaciones de protección de datos programadas, solo se registran los eventos de fallo de enlace en el registro de eventos (los eventos generados por las propias operaciones de protección de datos programadas aún se registran).

Orden de ejecución

Cuando se ejecuta una operación de protección de datos, los eventos de enlace de ejecución tienen lugar en el siguiente orden:

1. Los ganchos de ejecución de preoperación personalizados aplicables se ejecutan en los contenedores adecuados. Puede crear y ejecutar tantos ganchos de prefuncionamiento personalizados como necesite, pero el orden de ejecución de estos enlaces antes de la operación no está garantizado ni configurable.
2. Se realiza la operación de protección de datos.
3. Los enlaces de ejecución de post-operación personalizados aplicables se ejecutan en los contenedores adecuados. Puede crear y ejecutar tantos enlaces de post-operación personalizados como necesite, pero el orden de ejecución de estos enlaces después de la operación no está garantizado ni configurable.

Si crea varios enlaces de ejecución del mismo tipo (por ejemplo, presnapshot), no se garantiza el orden de ejecución de esos enlaces. Sin embargo, el orden de ejecución de ganchos de diferentes tipos está garantizado. Por ejemplo, el orden de ejecución de una configuración que tiene todos los diferentes tipos de ganchos se vería así:

1. Ganchos de precopia de seguridad ejecutados
2. Ganchos presnapshot ejecutados
3. Ganchos posteriores a la instantánea ejecutados
4. Se han ejecutado los enlaces posteriores a la copia de seguridad
5. Ganchos posteriores a la restauración ejecutados

Puede ver un ejemplo de esta configuración en el número de escenario 2 de la tabla de la Determine si se ejecutará un gancho.

> Siempre debe probar sus secuencias de comandos de ejecución de enlace antes de habilitarlas en un entorno de producción. Puede utilizar el comando 'kubectl exec' para probar cómodamente los scripts. Después de habilitar los enlaces de ejecución en un entorno de producción, pruebe las copias Snapshot y backups resultantes para garantizar que sean coherentes. Para ello, puede clonar la aplicación en un espacio de nombres temporal, restaurar la instantánea o la copia de seguridad y, a continuación, probar la aplicación.

Determine si se ejecutará un gancho

Utilice la siguiente tabla para determinar si se ejecutará un enlace de ejecución personalizado para su aplicación.

Tenga en cuenta que todas las operaciones de aplicaciones de alto nivel consisten en ejecutar una de las

operaciones básicas de copia Snapshot, backup o restauración. Según el supuesto, una operación de clonado puede consistir en diversas combinaciones de estas operaciones, de modo que lo que enlaza la ejecución de una operación de clonado será diferente.

Las operaciones de restauración sin movimiento requieren una snapshot o un backup existentes, por lo que estas operaciones no ejecutan datos instantáneos ni enlaces de backup.

> Si comienza pero luego cancela una copia de seguridad que incluye una instantánea y hay enlaces de ejecución asociados, es posible que se ejecuten algunos enlaces y es posible que otros no. Esto significa que un enlace de ejecución posterior a la copia de seguridad no puede suponer que la copia de seguridad se ha completado. Tenga en cuenta los siguientes puntos para realizar backups cancelados con enlaces de ejecución asociados:
>
> - Los enlaces de copia de seguridad previa y posterior siempre se ejecutan.
> - Si la copia de seguridad incluye una nueva instantánea y se ha iniciado la instantánea, se ejecutan los enlaces de preinstantánea y posterior a la instantánea.
> - Si la copia de seguridad se cancela antes del inicio de la instantánea, no se ejecutan los enlaces presnapshot y post snapshot.

Situación	Funcionamiento	Snapshot existente	Backup existente	Espacio de nombres	Clúster	Funcionan los enlaces de instantáneas	Funcionamiento de los ganchos de backup	Restaurar ejecución de ganchos
1	Clonar	N	N	Nuevo	Igual	Y	N	Y
2	Clonar	N	N	Nuevo	Diferente	Y	Y	Y
3	Clonar o restaurar	Y	N	Nuevo	Igual	N	N	Y
4	Clonar o restaurar	N	Y	Nuevo	Igual	N	N	Y
5	Clonar o restaurar	Y	N	Nuevo	Diferente	N	N	Y
6	Clonar o restaurar	N	Y	Nuevo	Diferente	N	N	Y
7	Restaurar	Y	N	Existente	Igual	N	N	Y
8	Restaurar	N	Y	Existente	Igual	N	N	Y
9	Snapshot	N.A.	N.A.	N.A.	N.A.	Y	N.A.	N.A.
10	Backup	N	N.A.	N.A.	N.A.	Y	Y	N.A.
11	Backup	Y	N.A.	N.A.	N.A.	N	N	N.A.

Ejemplos de gancho de ejecución

Visite la "Proyecto Verda GitHub de NetApp" Para descargar enlaces de ejecución real para aplicaciones populares como Apache Cassandra y Elasticsearch. También puede ver ejemplos y obtener ideas para estructurar sus propios enlaces de ejecución personalizados.

Active la función de enlaces de ejecución

Si es un usuario propietario o administrador, puede activar la función de enlaces de ejecución. Cuando habilita la función, todos los usuarios definidos en esta cuenta de Astra Control pueden usar ganchos de ejecución y ver los ganchos de ejecución y los scripts de enlace existentes.

Pasos

1. Vaya a **aplicaciones** y seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **ganchos de ejecución**.
3. Seleccione **Enable execution hooks**.

   Aparece la pestaña **Cuenta** > **Ajustes de función**.

4. En el panel * Ganchos de ejecución *, seleccione el menú de configuración.
5. Selecciona **Activar**.
6. Observe la advertencia de seguridad que aparece.
7. Seleccione **Sí, habilite los ganchos de ejecución**.

Desactive la función de enlaces de ejecución

Si eres un usuario propietario o administrador, puedes deshabilitar la función de enlaces de ejecución para todos los usuarios definidos en esta cuenta de Astra Control. Debe suprimir todos los enlaces de ejecución existentes antes de desactivar la función de enlaces de ejecución. Consulte Eliminar un gancho de ejecución para obtener instrucciones sobre cómo eliminar un enlace de ejecución existente.

Pasos

1. Vaya a **Cuenta** y luego seleccione la pestaña **Ajustes de función**.
2. Seleccione la ficha **ganchos de ejecución**.
3. En el panel * Ganchos de ejecución *, seleccione el menú de configuración.
4. Seleccione **Desactivar**.
5. Observe la advertencia que aparece.
6. Tipo `disable` para confirmar que desea deshabilitar la función para todos los usuarios.
7. Seleccione **Sí, desactivar**.

Ver los enlaces de ejecución existentes

Puede ver los enlaces de ejecución personalizados existentes para una aplicación.

Pasos

1. Vaya a **aplicaciones** y seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **ganchos de ejecución**.

   Puede ver todos los enlaces de ejecución habilitados o desactivados en la lista resultante. Puede ver el estado de un gancho, cuántos contenedores coinciden, la hora de creación y cuándo se ejecuta (antes o después de la operación). Puede seleccionar la + icono junto al nombre del gancho para expandir la lista de contenedores en los que se ejecutará. Para ver los registros de eventos que rodean los enlaces de ejecución de esta aplicación, vaya a la ficha **actividad**.

Ver los scripts existentes

Puede ver los scripts cargados existentes. También puede ver qué scripts están en uso, y qué enlaces los están utilizando, en esta página.

Pasos

1. Vaya a **cuenta**.
2. Seleccione la ficha **Scripts**.

   En esta página puede ver una lista de los scripts cargados existentes. La columna **Used by** muestra los enlaces de ejecución que utilizan cada script.

Agregar un script

Cada enlace de ejecución debe utilizar una secuencia de comandos para realizar acciones. Puede agregar una o más secuencias de comandos a las que puedan hacer referencia los enlaces de ejecución. Muchos ganchos de ejecución pueden hacer referencia al mismo script; esto le permite actualizar muchos ganchos de ejecución cambiando solo un script.

Pasos

1. Asegúrese de que la función de enlaces de ejecución es activado.
2. Vaya a **cuenta**.
3. Seleccione la ficha **Scripts**.
4. Seleccione **Agregar**.
5. Debe realizar una de las siguientes acciones:
   - Cargue un script personalizado.
     i. Seleccione la opción **cargar archivo**.
     ii. Navegue hasta un archivo y cárguelo.
     iii. Asigne al script un nombre único.
     iv. (Opcional) Introduzca cualquier nota que los otros administradores deben conocer sobre el script.
     v. Seleccione **Guardar script**.
   - Pegar en un script personalizado desde el portapapeles.
     i. Seleccione la opción **Pegar o Tipo**.
     ii. Seleccione el campo de texto y pegue el texto del script en el campo.
     iii. Asigne al script un nombre único.
     iv. (Opcional) Introduzca cualquier nota que los otros administradores deben conocer sobre el script.
6. Seleccione **Guardar script**.

Resultado

La nueva secuencia de comandos aparece en la lista de la ficha **Scripts**.

Eliminar un script

Puede eliminar una secuencia de comandos del sistema si ya no es necesaria y no se utiliza en ningún anzuelo de ejecución.

Pasos

1. Vaya a **cuenta**.
2. Seleccione la ficha **Scripts**.
3. Elija la secuencia de comandos que desee quitar y seleccione el menú en la columna **acciones**.
4. Seleccione **Eliminar**.

> Si la secuencia de comandos está asociada con uno o más enlaces de ejecución, la acción **Eliminar** no estará disponible. Para eliminar la secuencia de comandos, primero edite los enlaces de ejecución asociados y asócielos a una secuencia de comandos diferente.

Cree un enlace de ejecución personalizado

Puedes crear un gancho de ejecución personalizado para una aplicación y añadirlo a Astra Control. Consulte Ejemplos de gancho de ejecución para ejemplos de gancho. Necesita tener permisos de propietario, administrador o miembro para crear enlaces de ejecución.

> Cuando cree un script de shell personalizado para utilizarlo como un enlace de ejecución, recuerde especificar el shell adecuado al principio del archivo, a menos que esté ejecutando comandos específicos o proporcionando la ruta completa a un ejecutable.

Pasos

1. Asegúrese de que la función de enlaces de ejecución es activado.
2. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
3. Seleccione la ficha **ganchos de ejecución**.
4. Seleccione **Agregar**.
5. En el área **Detalles del gancho**:
   a. Determine cuándo debe funcionar el gancho seleccionando un tipo de operación en el menú desplegable **operación**.
   b. Introduzca un nombre único para el gancho.
   c. (Opcional) Introduzca cualquier argumento para pasar al gancho durante la ejecución, pulsando la tecla Intro después de cada argumento que introduzca para grabar cada uno.
6. (Opcional) en el área **Detalles de filtro de gancho**, puede añadir filtros para controlar en qué contenedores se ejecuta el gancho de ejecución:
   a. Seleccione **Agregar filtro**.
   b. En la columna **Tipo de filtro Hook**, elija un atributo en el que filtrar en el menú desplegable.
   c. En la columna **Regex**, introduzca una expresión regular que se utilizará como filtro. Astra Control utiliza "Sintaxis de regex de expresión regular 2 (RE2)".

      > Si filtra el nombre exacto de un atributo (como un nombre de POD) sin ningún otro texto en el campo de expresión normal, se realizará una coincidencia de subcadena. Para que coincida con un nombre exacto y sólo con ese nombre, utilice la sintaxis de coincidencia de cadena exacta (por ejemplo, `^exact_podname$`).

   d. Para añadir más filtros, seleccione **Agregar filtro**.

> Se combinan varios filtros para un enlace de ejecución con un operador y lógico. Puede tener hasta 10 filtros activos por gancho de ejecución.

7. Cuando termine, seleccione **Siguiente**.
8. En el área **Script**, siga uno de estos procedimientos:
   - Agregue un nuevo script.
     i. Seleccione **Agregar**.
     ii. Debe realizar una de las siguientes acciones:
       - Cargue un script personalizado.
         I. Seleccione la opción **cargar archivo**.
         II. Navegue hasta un archivo y cárguelo.
         III. Asigne al script un nombre único.
         IV. (Opcional) Introduzca cualquier nota que los otros administradores deben conocer sobre el script.
         V. Seleccione **Guardar script**.
       - Pegar en un script personalizado desde el portapapeles.
         I. Seleccione la opción **Pegar o Tipo**.
         II. Seleccione el campo de texto y pegue el texto del script en el campo.
         III. Asigne al script un nombre único.
         IV. (Opcional) Introduzca cualquier nota que los otros administradores deben conocer sobre el script.
   - Seleccione un script existente de la lista.

     Esto indica al enlace de ejecución que utilice esta secuencia de comandos.
9. Seleccione **Siguiente**.
10. Revise la configuración del gancho de ejecución.
11. Seleccione **Agregar**.

Compruebe el estado de un enlace de ejecución

Después de que una operación de instantánea, backup o restauración finalice la ejecución, puede comprobar el estado de los enlaces de ejecución que se ejecutan como parte de la operación. Puede utilizar esta información de estado para determinar si desea mantener el enlace de ejecución, modificarlo o eliminarlo.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **Protección de datos**.
3. Seleccione **instantáneas** para ver las instantáneas en ejecución, o **copias de seguridad** para ver las copias de seguridad en ejecución.

   El estado * gancho* muestra el estado de la ejecución del gancho de ejecución una vez completada la operación. Puede pasar el ratón sobre el estado para obtener más detalles. Por ejemplo, si hay fallos de enlace de ejecución durante una instantánea, pasar el ratón sobre el estado de enlace de esa instantánea proporciona una lista de los enlaces de ejecución fallidos. Para ver las razones de cada fallo, puede

consultar la página **actividad** en el área de navegación del lado izquierdo.

Ver el uso de las secuencias de comandos

Puede ver qué enlaces de ejecución utilizan una secuencia de comandos determinada en la interfaz de usuario web de Astra Control.

Pasos

1. Seleccione **cuenta**.
2. Seleccione la ficha **Scripts**.

   La columna **usado por** de la lista de scripts contiene detalles sobre qué ganchos están utilizando cada script de la lista.

3. Seleccione la información de la columna **utilizado por** para un script que le interese.

   Aparece una lista más detallada, con los nombres de los ganchos que utilizan la secuencia de comandos y el tipo de operación con la que están configurados para ejecutarse.

Edite un gancho de ejecución

Puede editar un enlace de ejecución si desea cambiar sus atributos, filtros o la secuencia de comandos que utiliza. Necesita tener permisos de propietario, administrador o miembro para editar los enlaces de ejecución.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **ganchos de ejecución**.
3. Seleccione el menú Opciones de la columna **acciones** para un gancho que desee editar.
4. Seleccione **Editar**.
5. Haga los cambios necesarios, seleccione **Siguiente** después de completar cada sección.
6. Seleccione **Guardar**.

Desactivar un gancho de ejecución

Puede desactivar un gancho de ejecución si desea impedir temporalmente que se ejecute antes o después de una instantánea de una aplicación. Necesita tener permisos de propietario, administrador o miembro para desactivar los enlaces de ejecución.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **ganchos de ejecución**.
3. Seleccione el menú Opciones de la columna **acciones** para el gancho que desea desactivar.
4. Seleccione **Desactivar**.

Eliminar un gancho de ejecución

Puede eliminar un enlace de ejecución por completo si ya no lo necesita. Necesita tener permisos de propietario, administrador o miembro para eliminar los enlaces de ejecución.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **ganchos de ejecución**.
3. Seleccione el menú Opciones de la columna **acciones** para el gancho que desea eliminar.
4. Seleccione **Eliminar**.
5. En el cuadro de diálogo que aparece, escriba "delete" para confirmar.
6. Seleccione **Sí, elimine el enlace de ejecución**.

Si quiere más información

- "Proyecto Verda GitHub de NetApp"

Ver el estado de las aplicaciones y la computación

Ver un resumen del estado de las aplicaciones y el clúster

Haga clic en * Dashboard* para ver una vista de alto nivel de sus aplicaciones, clusters y su estado de salud.

El icono aplicaciones le ayuda a identificar lo siguiente:

- ¿Cuántas aplicaciones gestiona actualmente?
- Si esas aplicaciones gestionadas están en buen estado.
- Si las aplicaciones están totalmente protegidas (están protegidas si hay backups recientes disponibles).

Tenga en cuenta que no se trata sólo de números o Estados, sino que puede obtener información detallada de cada uno de ellos. Por ejemplo, si las aplicaciones no están completamente protegidas, puede pasar el ratón sobre el icono para identificar qué aplicaciones no están completamente protegidas, lo que incluye un motivo.

El icono clústeres ofrece detalles similares sobre el estado del clúster y es posible profundizar para obtener más detalles como puede hacerlo con una aplicación.

Consulte el estado y los detalles de los clústeres

Después de añadir clústeres de Kubernetes a Astra Control, puede ver detalles sobre el clúster, como su ubicación, los nodos de trabajo, los volúmenes persistentes y las clases de almacenamiento.

Pasos

1. En la interfaz de usuario de Astra Control Service, seleccione **Clusters**.
2. En la página **Clusters**, seleccione el clúster cuyos detalles desea ver.

> Si hay un clúster en `removed` estado aunque la conectividad del clúster y de la red parece correcta (los intentos externos de acceder al clúster mediante las API de Kubernetes se han realizado correctamente), es posible que la imagen que proporcionó a Astra Control ya no sea válida. Esto puede deberse a la rotación o a la caducidad del certificado en el clúster. Para corregir este problema, actualice las credenciales asociadas con el clúster en Astra Control mediante "API de control Astra".

3. Consulte la información en las pestañas **Descripción general**, **almacenamiento** y **actividad** para encontrar la información que busca.
   - **Descripción general**: Detalles sobre los nodos de trabajo, incluido su estado.
   - **almacenamiento**: Los volúmenes persistentes asociados con el cálculo, incluyendo la clase de almacenamiento y el estado.
   - **Actividad**: Las actividades relacionadas con el cluster.

> También puede ver la información del clúster empezando por Astra Control Service **Dashboard**. En la ficha **Clusters** de **Resumen de recursos**, puede seleccionar los clústeres administrados, que le llevará a la página **Clusters**. Después de llegar a la página **Clusters**, siga los pasos descritos anteriormente.

Ver el estado y los detalles de una aplicación

Después de empezar a gestionar una aplicación, Astra Control proporciona detalles sobre la aplicación que te permiten identificar el estado de comunicación (si Astra Control puede comunicarse con la aplicación), su estado de protección (si está totalmente protegido en caso de fallo), los pods, el almacenamiento persistente y mucho más.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. Encuentre la información que busca:

   Estado de la aplicación

   Proporciona un estado que refleja si Astra Control puede comunicarse con la aplicación.

   Estado de protección de aplicaciones

   Proporciona el estado de la protección de la aplicación:

   - **totalmente protegido**: La aplicación tiene una programación de copia de seguridad activa y una copia de seguridad exitosa que tiene menos de una semana de antigüedad
   - **parcialmente protegido**: La aplicación tiene una programación de copia de seguridad activa, una programación de instantáneas activa o una copia de seguridad o instantánea correcta
   - **desprotegido**: Aplicaciones que no están completamente protegidas o parcialmente protegidas.

     no puede estar completamente protegido hasta que tenga una copia de seguridad reciente. Esto es importante porque los backups se almacenan en un almacén de objetos lejos de los volúmenes persistentes. Si un fallo o accidente limpia el cluster y es almacenamiento persistente, necesitará una copia de seguridad para recuperar. Una Snapshot no le permite recuperar.

   Descripción general

   Información sobre el estado de los pods asociados con la aplicación.

   Protección de datos

   Permite configurar una política de protección de datos y ver las Snapshot y los backups existentes.

   Reducida

   Muestra los volúmenes persistentes a nivel de aplicación. El estado de un volumen persistente es desde el punto de vista del clúster de Kubernetes.

Recursos

Permite verificar qué recursos se están gestionando y haciendo backup.

Actividad

Las actividades de Astra Control relacionadas con la app.

Gestionar bloques

Puede gestionar los bloques que Astra utiliza para backups y clones. Puede añadir bloques adicionales, quitar bloques existentes y cambiar el bloque predeterminado para los clústeres de Kubernetes en una instancia de cloud.

Solo los propietarios y administradores pueden gestionar los bloques.

Cómo utiliza el control Astra cucharones

Cuando empiece a gestionar su primer clúster Kubernetes para una instancia de cloud, Astra Control Service crea el bloque inicial para este fin "instancia de cloud".

Puede designar manualmente un bloque como el bloque predeterminado para una instancia de cloud. Si lo hace, Astra Control Service utiliza este bloque de forma predeterminada para las copias de seguridad y clones que cree en cualquier clúster gestionado de esa instancia cloud (puede seleccionar un bloque diferente para las copias de seguridad). Si clona una aplicación en vivo desde cualquiera de los clústeres gestionados de una instancia de cloud a otro clúster, Astra Control Service utiliza el bloque predeterminado para la instancia de cloud de origen para realizar la operación de clonado.

Puede establecer el mismo bloque que el bloque predeterminado para varias instancias de cloud.

Puede seleccionar desde cualquier grupo cuando crea una política de protección o inicia un backup ad hoc.

> El servicio Astra Control Service comprueba si se puede acceder a un bloque de destino antes de iniciar una copia de seguridad o un clon.

Ver los bloques existentes

Consulte la lista de bloques disponibles para Astra Control Service para determinar su estado e identificar el bloque predeterminado (si se ha definido) para su instancia de cloud.

Un bloque puede tener cualquiera de los siguientes estados:

Pendiente

Después de añadir un cucharón, se inicia en el estado pendiente mientras Astra Control lo detecta.

Disponible

El cucharón está disponible para su uso por Astra Control.

Quitada

La cuchara no está operativa por el momento. Pase el ratón sobre el icono de estado para identificar el problema.

Si un bloque se encuentra en el estado quitado, puede establecerlo como el bloque predeterminado y

asignarlo a un programa de protección. Pero si el bloque no está en estado disponible cuando se inicia una operación de protección de datos, esta operación falla.

Paso

1. Vaya a **Cuchos**.

   Se muestra la lista de cucharones disponibles para el servicio de control de Astra.

Añadir un bloque más

Puede añadir cubos adicionales en cualquier momento. Esto le permite elegir entre bloques al crear una política de protección o iniciar un backup ad hoc, y le permite cambiar el bloque predeterminado que utiliza una instancia de cloud.

Puede añadir los siguientes tipos de cubos:

- Amazon Web Services
- Genérico S3
- Google Cloud Platform
- Microsoft Azure
- ONTAP S3 de NetApp
- StorageGRID S3 de NetApp

Antes de empezar

- Asegúrese de conocer el nombre de un depósito existente.
- Asegúrate de tener credenciales para el bloque que proporcionan a Astra Control los permisos que necesita para gestionar el bloque.
- Si su bloque está en Microsoft Azure:
  - El bloque debe pertenecer al grupo de recursos denominado *astra-backup-rg*.
  - Si la configuración del rendimiento de la instancia de la cuenta de almacenamiento de Azure se establece en "Premium", la opción "Tipo de cuenta Premium" debe configurarse en "Block Blobs".

Pasos

1. Vaya a **Cuchos**.
2. Seleccione **Agregar** y siga las indicaciones para añadir el cucharón.
   - **Tipo**: Elija su proveedor de nube.
   - **Nombre del cucharón existente**: Introduzca el nombre del cucharón.
   - **Descripción**: Si lo desea, introduzca una descripción del cucharón.
     - **Cuenta de almacenamiento** (sólo Azure): Introduzca el nombre de su cuenta de almacenamiento de Azure. Este bloque debe pertenecer al grupo de recursos denominado *astra-backup-rg*.
     - **Nombre de servidor S3 o dirección IP** (sólo tipos de bloques AWS y S3): Introduzca el nombre de dominio completo del extremo S3 que corresponda a su región, sin `https://`. Consulte "La documentación de Amazon" si quiere más información.
     - **Seleccionar credenciales**: Introduzca las credenciales que proporcionan a Astra Control Service los permisos que necesita para administrar el bloque. La información que debe proporcionar varía en función del tipo de segmento.

a. Seleccione **Agregar** para añadir el cucharón.

Resultado

Astra Control Service añade el cucharón. Ahora puede elegir este bloque cuando cree una política de protección o ejecute un backup ad hoc. También puede establecer este bloque como el bloque predeterminado para una instancia de cloud.

Cambiar el bloque predeterminado

Puede cambiar el bloque predeterminado para una instancia de cloud. Astra Control Service utilizará este bloque de forma predeterminada para las copias de seguridad y clones. Cada instancia de cloud tiene su propio bloque predeterminado.

> Astra Control no asigna automáticamente un bloque predeterminado para ninguna instancia de cloud. Debe establecer manualmente un bloque predeterminado para una instancia de cloud antes de ejecutar operaciones de clonado de aplicaciones entre dos clústeres.

Pasos

1. Vaya a **instancias de cloud**.
2. Seleccione el menú de configuración de la columna **acciones** para la instancia de nube que desea editar.
3. Seleccione **Editar**.
4. En la lista de bloques, seleccione el bloque que desea convertir en el bloque predeterminado para esta instancia de cloud.
5. Seleccione **Actualizar**.

Retirar un cucharón

Puede eliminar un cubo que ya no esté en uso o que no esté sano. Se recomienda hacer esto para mantener la configuración del almacén de objetos sencilla y actualizada.

> - No se puede eliminar un bloque predeterminado. Si desea eliminar ese bloque, seleccione primero otro bloque como predeterminado.
> - No puede quitar un depósito de escritura única y lectura múltiple (WORM) antes de que haya caducado el período de retención del proveedor de cloud del depósito. Los depósitos WORM están marcados con «bloqueados» junto al nombre del bloque.

Antes de empezar

- Antes de empezar, debe comprobar que no hay copias de seguridad en ejecución o completadas para este bloque.
- Debe comprobar que dicho bloque no se esté utilizando para ninguna copia de seguridad programada.

Si lo hay, no podrá continuar.

Pasos

1. Vaya a **Cuchos**.
2. En el menú **acciones**, seleccione **Quitar**.

> Astra Control garantiza en primer lugar que no existan normativas de programación utilizando el bloque para copias de seguridad y que no haya copias de seguridad activas en el bloque que va a eliminar.

3. Escriba "eliminar" para confirmar la acción.
4. Seleccione **Sí, retire la cuchara**.

[Vista PREVIA TÉCNICA] Gestione un bloque con un recurso personalizado

Puede añadir un bloque con un recurso personalizado de Astra Control (CR) en el clúster de aplicaciones. Añadir proveedores de bloques de almacenamiento de objetos es esencial si desea realizar backups de sus aplicaciones y del almacenamiento persistente o si desea clonar aplicaciones entre clústeres. Astra Control almacena estas copias de seguridad o clones en los bloques de almacenamiento de objetos que defina. Si utiliza el método de recursos personalizado, la funcionalidad de snapshots de aplicaciones requiere un bloque.

No necesita un bloque de Astra Control si clona la configuración de sus aplicaciones y el almacenamiento persistente en el mismo clúster.

El recurso personalizado de bloque para Astra Control se conoce como AppVault. Este CR contiene las configuraciones necesarias para que un cucharón se utilice en operaciones de protección.

Antes de empezar

- Asegúrese de tener un bloque al que se puede acceder desde los clústeres que gestiona Astra Control Center.
- Asegúrese de tener credenciales para el bloque.
- Asegúrese de que el cucharón es uno de los siguientes tipos:
  - ONTAP S3 de NetApp
  - StorageGRID S3 de NetApp
  - Microsoft Azure
  - Genérico S3

> Amazon Web Services (AWS) y Google Cloud Platform (GCP) utilizan el tipo de bloque Generic S3.

> Aunque Astra Control Center es compatible con Amazon S3 como proveedor de bloques Generic S3, es posible que Astra Control Center no admita todos los proveedores de almacenes de objetos que afirman que Amazon es compatible con S3.

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre (por ejemplo, `astra-appvault.yaml`).
2. Configure los siguientes atributos:
   - **metadata.name**: *(required)* El nombre del recurso personalizado de AppVault.
   - **Spec.prefix**: *(Opcional)* Una ruta que tiene el prefijo de los nombres de todas las entidades almacenadas en AppVault.
   - **spec.providerConfig**: *(required)* Almacena la configuración necesaria para acceder a AppVault

utilizando el proveedor especificado.

- **spec.providerCredentials**: *(required)* Almacena referencias a cualquier credencial necesaria para acceder a AppVault utilizando el proveedor especificado.
  - **spec.providerCredentials.valueFromSecret**: *(Opcional)* indica que el valor de la credencial debe provenir de un secreto.
    - **KEY**: *(requerido si se usa valueFromSecret)* La clave válida del secreto para seleccionar.
    - **Name**: *(requerido si se usa valueFromSecret)* Nombre del secreto que contiene el valor de este campo. Debe estar en el mismo espacio de nombres.
- **spec.providerType**: *(required)* Determina qué proporciona la copia de seguridad; por ejemplo, NetApp ONTAP S3 o Microsoft Azure.

Ejemplo YAML:

```yaml
apiVersion: astra.netapp.io/v1
kind: AppVault
metadata:
  name: astra-appvault
spec:
  providerType: generic-s3
  providerConfig:
    path: testpath
    endpoint: 192.168.1.100:80
    bucketName: bucket1
    secure: "false"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        name: s3-creds
        key: accessKeyID
    secretAccessKey:
      valueFromSecret:
        name: s3-creds
        key: secretAccessKey
```

3. Después de rellenar el `astra-appvault.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -f astra-appvault.yaml -n astra-connector
```

> Cuando se agrega un bloque, Astra Control Marca un bloque con el indicador de segmento predeterminado. El primer bloque que crea se convierte en el bloque predeterminado. A medida que se añaden bloques, más adelante se puede decidir a. "establecer otro bloque predeterminado".

Obtenga más información

- "Utilice la API Astra Control"

Supervisar tareas en ejecución

Puede ver detalles sobre las tareas en ejecución y las tareas que se han completado, han fallado o han sido canceladas en las últimas 24 horas en Astra Control. Por ejemplo, puede ver el estado de una operación de backup, restauración o clonado en ejecución, y ver detalles como un porcentaje completado y el tiempo restante estimado. Es posible ver el estado de una operación programada que se haya ejecutado o una operación que se inició manualmente.

Mientras ve una tarea en ejecución o completada, puede expandir los detalles de la tarea para ver el estado de cada una de las subtareas. La barra de progreso de la tarea es verde para las tareas en curso o completadas, azul para las tareas canceladas y rojo para las tareas que han fallado debido a un error.

> Para las operaciones de clonado, las subtareas consisten en una operación de restauración de Snapshot y de Snapshot.

Para obtener más información sobre las tareas que han fallado, consulte "Controlar la actividad de la cuenta".

Pasos

1. Mientras se está ejecutando una tarea, vaya a **aplicaciones**.
2. Seleccione el nombre de una aplicación de la lista.
3. En los detalles de la aplicación, seleccione la ficha **tareas**.

   Puede ver detalles de tareas actuales o pasadas y filtrar por estado de tarea.

> Las tareas se conservan en la lista **tareas** durante un máximo de 24 horas. Puede configurar este límite y otros ajustes del monitor de tareas mediante "API de control Astra".

Gestione su cuenta

Configurar facturación

Puede utilizar más de un método para gestionar la facturación de su cuenta de Astra Control Service. Si utiliza Azure o Amazon AWS, puede suscribirse a un plan de servicio Astra Control a través de Microsoft Azure Marketplace o AWS Marketplace. Al hacerlo, puede gestionar sus datos de facturación a través del mercado. O bien, puede suscribirse directamente a NetApp. Si se suscribe directamente con NetApp, puede gestionar los datos de su facturación a través del servicio Astra Control Service. Si utiliza Astra Control Service sin suscripción, se suscribiera automáticamente al plan gratuito.

El plan gratuito de Astra Control Service le permite gestionar hasta 10 espacios de nombres en su cuenta. Si desea gestionar más de 10 espacios de nombres, debe configurar la facturación mediante la actualización del plan gratuito al plan Premium, o bien suscribirse a través de Azure Marketplace o AWS Marketplace.

Descripción general de la facturación

Existen dos tipos de costes asociados con el uso de Astra Control Service: Cargos por parte de NetApp por el Servicio Astra Control y cargos por parte de su proveedor de cloud por volúmenes persistentes y almacenamiento de objetos.

Facturación de Astra Control Service

Astra Control Service ofrece tres planes:

Plan libre
: Gestione hasta 10 espacios de nombres de forma gratuita.

Premium PAYGO
: Gestione una cantidad ilimitada de espacios de nombres a una tasa específica, por espacio de nombres.

Suscripción Premium
: Prepago a una tarifa con descuento con una suscripción anual que le permite administrar hasta 20 espacios de nombres por *paquete de espacio de nombres*. Póngase en contacto con el departamento de ventas de NetApp para adquirir tantos paquetes como necesite para su organización. Por ejemplo, compre 3 paquetes para gestionar 60 espacios de nombres desde Astra Control Service. Si gestiona más espacios de nombres de los permitidos en su suscripción anual, se le cobrará la tasa de exceso dependiente de la suscripción por espacio de nombres adicional. Si aún no dispone de una cuenta de Astra Control, al adquirir la suscripción Premium, se crea automáticamente una cuenta de Astra Control para usted. Si ya dispone de un plan gratuito, se convertirá automáticamente a la suscripción Premium.

Al crear una cuenta de Astra Control, se suscribe automáticamente al Plan libre. El panel de control de Astra muestra cuántos espacios de nombres gestiona actualmente con los 10 espacios de nombres gratuitos que está permitido. La facturación se inicia para un espacio de nombres cuando se gestiona la primera aplicación que contiene el espacio de nombres y se detiene para ese espacio de nombres cuando no se gestiona la última aplicación que contiene el espacio de nombres.

Si intenta gestionar un espacio de nombres 11, Astra Control le notifica que ha alcanzado el límite del Plan libre. A continuación, le pedirá que actualice el plan gratuito a un plan Premium. Se le cobrará la tasa de exceso dependiente de la suscripción por espacio de nombres adicional.

Puede actualizar a un plan Premium en cualquier momento. Después de actualizar, Astra Control comienza a cobrarle por espacios de nombres *all* en la cuenta. Los primeros 10 espacios de nombres no se quedan en el plan gratuito.

Facturación de Google Cloud

Los volúmenes persistentes están respaldados por NetApp Cloud Volumes Service y los backups de tus aplicaciones se almacenan en un depósito de Google Cloud Storage.

- "Consulte los detalles de precios para Cloud Volumes Service".

  Tenga en cuenta que Astra Control Service es compatible con todos los tipos de servicio y niveles de servicio. El tipo de servicio que utilice dependerá de su "Región de Google Cloud".

- "Vea los detalles de precios para buckets de almacenamiento de Google Cloud".

Facturación de Microsoft Azure

Azure NetApp Files respalda los volúmenes persistentes y los backups de tus aplicaciones se almacenan en un contenedor de Azure Blob.

- "Consulte los detalles de precios para Azure NetApp Files".
- "Consulte los detalles de precios para el almacenamiento de Microsoft Azure Blob".
- "Consulta los planes y los precios del servicio de Astra Control en Azure Marketplace"

> La tasa de facturación de Azure para Astra Control Service es por hora y una nueva hora de facturación se inicia después de que hayan transcurrido 29 minutos de la hora de uso.

Facturación de Amazon Web Services

Los volúmenes persistentes están respaldados por EBS o FSx para NetApp ONTAP, y los backups de tus aplicaciones se almacenan en un bucket de AWS.

- "Consulte los detalles de precios de Amazon Web Services".

Suscríbase al servicio Astra Control Service en Azure Marketplace

Puede suscribirse al servicio Astra Control Service mediante Azure Marketplace. La cuenta y los datos de facturación se gestionan a través del Marketplace.

> Para ver un tutorial en vídeo del proceso de suscripción a Azure Marketplace, visite "TV de NetApp".

Pasos

1. Vaya a la "Azure Marketplace".
2. Seleccione **Get It Now**.
3. Siga las instrucciones para suscribirse a un plan.

Suscríbase al servicio Astra Control Service en AWS Marketplace

Puede suscribirse al servicio Astra Control Service mediante AWS Marketplace. La cuenta y los datos de facturación se gestionan a través del Marketplace.

Pasos

1. Vaya a la "Mercado AWS".
2. Seleccione **Ver opciones de compra**.
3. Si se le solicita hacerlo, inicie sesión en su cuenta de AWS o cree una nueva cuenta.
4. Siga las instrucciones para suscribirse a un plan.

Suscríbase al servicio Astra Control directamente con NetApp

Puede suscribirse al servicio Astra Control Service desde la interfaz de usuario del servicio Astra Control o ponerse en contacto con las ventas de NetApp.

Mejora del plan gratuito al plan Premium PAYGO

Actualice su plan de facturación en cualquier momento para comenzar a gestionar más de 10 espacios de nombres de Astra Control pagando a medida que usted va. Todo lo que necesitas es una tarjeta de crédito válida.

Pasos

1. Seleccione **cuenta** y, a continuación, seleccione **facturación**.
2. En **planes**, vaya a **Premium PAYGO** y seleccione **Actualizar ahora**.
3. Proporcione los datos de pago de una tarjeta de crédito válida y seleccione **Actualizar a Plan Premium**.

> Astra Control le enviará por correo electrónico si la tarjeta de crédito está a punto de expirar.

Resultado

Ahora puede gestionar más de 10 espacios de nombres. Astra Control comienza a cobrarle por los espacios de nombres *All* que está administrando actualmente.

Actualice del plan gratuito a la suscripción Premium

Póngase en contacto con el equipo de ventas de NetApp para solicitar un pago con tarifa con descuento con una suscripción anual.

Pasos

1. Seleccione **cuenta** y, a continuación, seleccione **facturación**.
2. En **planes**, vaya a **Suscripción Premium** y seleccione **Ventas de contacto**.
3. Facilite los detalles al equipo de ventas para comenzar el proceso.

Resultado

Un representante de ventas de NetApp se pondrá en contacto con usted para procesar su pedido de compra. Una vez completado el pedido, Astra Control reflejará su plan actual en la pestaña **facturación**.

Ver los costes actuales y el historial de facturación

Astra Control le muestra sus costes mensuales actuales, así como un historial detallado de facturación por espacio de nombres. Si se suscribe a un plan a través de un mercado, el historial de facturación no está visible (pero puede verlo iniciando sesión en el mercado).

Pasos

1. Seleccione **cuenta** y, a continuación, seleccione **facturación**.

   Sus costos actuales aparecen bajo la descripción general de la facturación.

2. Para ver el historial de facturación por espacio de nombres, seleccione **Historial de facturación**.

   Astra Control le muestra los minutos de uso y los costes de cada espacio de nombres. Un minuto de uso es cuántos minutos Astra Control ha gestionado su espacio de nombres durante un periodo de facturación.

3. Seleccione la lista desplegable para seleccionar un mes anterior.

Cambie la tarjeta de crédito de Premium PAYGO

Si es necesario, puede cambiar la tarjeta de crédito que Astra Control tiene en el archivo para la facturación.

Pasos

1. Seleccione **cuenta > facturación > método de pago**.
2. Seleccione el icono de configuración.
3. Modificar la tarjeta de crédito.

Notas importantes

- Su plan de facturación se realiza por cuenta Astra Control.

  Si tiene varias cuentas, cada una tiene su propio plan de facturación.

- La factura de Astra Control incluye cargos por la gestión de sus espacios de nombres. Su proveedor de cloud lo carga por separado para el back-end de almacenamiento de volúmenes persistentes.

  "Más información sobre los precios de Astra Control".

- Cada período de facturación finaliza el último día del mes.
- No puede cambiar de un plan Premium a un plan gratuito.

Invitar y quitar usuarios

Invite a los usuarios a unirse a su cuenta de Astra Control y eliminar usuarios que ya no deberían tener acceso a la cuenta.

Invitar a los usuarios

Los propietarios y administradores de cuentas pueden invitar a otros usuarios a unirse a la cuenta de Astra Control.

Pasos

1. Asegúrese de que el usuario tiene un "Inicio de sesión de BlueXP".
2. Seleccione **cuenta**.
3. En la ficha **usuarios**, seleccione **Invitar**.
4. Introduzca el nombre del usuario, la dirección de correo electrónico y el rol.

   Tenga en cuenta lo siguiente:

   - La dirección de correo electrónico debe coincidir con la dirección de correo electrónico que el usuario usó para registrarse en BlueXP.
   - Cada rol proporciona los siguientes permisos:
     - Un **propietario** tiene permisos de administrador y puede eliminar cuentas.
     - Un **Admin** tiene permisos de miembro y puede invitar a otros usuarios.
     - Un **Miembro** puede administrar completamente aplicaciones y clústeres.
     - Un **Visor** puede ver los recursos.

5. Para agregar restricciones a un usuario con un rol de miembro o de visor, active la casilla de verificación **restringir la función a restricciones** .

   Para obtener más información sobre cómo agregar restricciones, consulte "Gestionar roles".

6. Para invitar a otro usuario, seleccione **Añadir otro usuario** e introduzca información para el nuevo usuario.

   Puede invitar hasta 10 usuarios a la vez. Puede navegar entre los usuarios a los que está invitando en el lado izquierdo del diálogo **Invitar usuarios**.

7. Seleccione **Invitar usuarios**.

Resultado

El usuario o los usuarios recibirán un correo electrónico que les invita a unirse a su cuenta.

Cambiar el rol de un usuario

Un propietario de cuenta puede cambiar la función de todos los usuarios, mientras que un administrador de cuenta puede cambiar la función de los usuarios que tienen la función Admin, Miembro o Visor.

Pasos

1. Seleccione **cuenta**.
2. En la ficha **usuarios**, seleccione el menú en la columna **acciones** del usuario.
3. Seleccione **Editar rol**.
4. Seleccione un rol nuevo.
5. Para agregar restricciones a un usuario con un rol de miembro o de visor, active la casilla de verificación **restringir la función a restricciones** .

   Para obtener más información sobre cómo agregar restricciones, consulte "Gestionar roles".

6. Seleccione **Confirmar**.

Resultado

Astra Control actualiza los permisos del usuario en función de la nueva función que haya seleccionado.

Quitar usuarios

Un usuario con el rol propietario puede eliminar otros usuarios de la cuenta en cualquier momento.

Pasos

1. Seleccione **cuenta**.
2. En la ficha **usuarios**, seleccione los usuarios que desea quitar.
3. Seleccione el menú en la columna **acciones** y seleccione **Eliminar usuario**.
4. Cuando se le solicite, confirme la eliminación escribiendo "eliminar" y, a continuación, seleccione **Sí, Eliminar usuario**.

Resultado

Astra Control elimina al usuario de la cuenta.

Gestionar roles

Es posible gestionar roles si se añaden restricciones de espacio de nombres y se restringen los roles del usuario a dichas restricciones. Esto le permite controlar el acceso a los recursos de su organización. Puede utilizar la interfaz de usuario de Astra Control o. "La API de control Astra" para administrar roles.

Agregar una restricción de espacio de nombres a una función

Un usuario Admin o Owner puede agregar restricciones de espacio de nombres.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **usuarios**.
3. En la columna **acciones**, seleccione el botón de menú para un usuario con la función Miembro o Visor.
4. Seleccione **Editar rol**.
5. Active la casilla de verificación **restringir rol a restricciones**.

   La casilla de verificación sólo está disponible para funciones de miembro o de visor. Puede seleccionar un rol diferente de la lista desplegable **rol**.

6. Seleccione **Agregar restricción**.

   Se puede ver la lista de restricciones disponibles por espacio de nombres o por etiqueta de espacio de nombres.

7. En la lista desplegable **Tipo de restricción**, seleccione **espacio de nombres Kubernetes** o **etiqueta de espacio de nombres Kubernetes** dependiendo de cómo estén configurados los espacios de nombres.
8. Seleccione uno o más espacios de nombres o etiquetas de la lista para redactar una restricción que restrinja las funciones a esos espacios de nombres.
9. Seleccione **Confirmar**.

   La página **Editar función** muestra la lista de restricciones que ha elegido para esta función.

10. Seleccione **Confirmar**.

    En la página **cuenta**, puede ver las restricciones de cualquier rol de miembro o de visor en la columna **rol**.

> Si habilita restricciones para una función y selecciona **Confirmar** sin agregar restricciones, se considera que la función tiene restricciones completas (se deniega el acceso a cualquier recurso asignado a espacios de nombres).

Quitar una restricción de espacio de nombres de una función

Un usuario Admin o Owner puede eliminar una restricción de espacio de nombres de una función.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **usuarios**.

3. En la columna **acciones**, seleccione el botón de menú para un usuario con la función Miembro o Visor que tiene restricciones activas.
4. Seleccione **Editar rol**.

   El cuadro de diálogo **Editar función** muestra las restricciones activas para la función.

5. Seleccione **X** a la derecha de la restricción que debe eliminar.
6. Seleccione **Confirmar**.

Si quiere más información

- "Roles de usuario y espacios de nombres"

Añada y elimine credenciales

Añada y elimine credenciales de proveedor de cloud de su cuenta en cualquier momento. Astra Control utiliza estas credenciales para descubrir un clúster de Kubernetes, las aplicaciones en el clúster y aprovisionar recursos en su nombre.

Tenga en cuenta que todos los usuarios de Astra Control comparten los mismos conjuntos de credenciales.

Añada credenciales

La forma más común de agregar credenciales a Astra Control es cuando se gestionan los clústeres, pero también se pueden añadir credenciales desde la página cuenta. De ese modo, las credenciales estarán disponibles para elegir cuando gestione clústeres de Kubernetes adicionales.

Antes de empezar

- Para Amazon Web Services, debe tener el resultado JSON de las credenciales de la cuenta IAM que se utiliza para crear el clúster. "Aprenda a configurar un usuario de IAM".
- Para GKE, debe tener el archivo de clave de cuenta de servicio para una cuenta de servicio que tenga los permisos necesarios. "Aprenda a configurar una cuenta de servicio".
- Para AKS, debe tener el archivo JSON que contenga el resultado de la CLI de Azure cuando creó el principal de servicio. "Aprenda a configurar un director de servicios".

  También necesitará su ID de suscripción de Azure si no lo ha añadido al archivo JSON.

Pasos

1. Seleccione **cuenta > credenciales**.
2. Seleccione **Agregar credenciales**.
3. Seleccione **Microsoft Azure**.
4. Seleccione **Google Cloud Platform**.
5. Seleccione **Amazon Web Services**.
6. Introduzca un nombre para las credenciales que las distinga de otras credenciales en Astra Control.
7. Proporcione las credenciales necesarias.
8. **Microsoft Azure**: Proporcione a Astra Control detalles sobre el principal de servicio de Azure cargando un archivo JSON o pegando el contenido de ese archivo JSON desde el portapapeles.

El archivo JSON debe contener el resultado de la CLI de Azure al crear el principal del servicio. También puede incluir su ID de suscripción para que se agregue automáticamente a Astra Control. De lo contrario, deberá introducir manualmente el ID después de proporcionar JSON.

9. **Google Cloud Platform**: Proporcione el archivo clave de la cuenta de servicio de Google Cloud mediante la carga del archivo o pegando el contenido del portapapeles.
10. **Amazon Web Services**: Proporcione las credenciales de usuario de IAM de Amazon Web Services cargando el archivo o pegando el contenido del portapapeles.
11. Seleccione **Agregar credenciales**.

Resultado

Las credenciales ahora están disponibles para seleccionar cuando agregue un clúster a Astra Control.

Quite las credenciales

Eliminar credenciales de una cuenta en cualquier momento. Solo debe quitar credenciales después de "desgestione todos los clústeres", a menos que esté rotando credenciales (consulte Rotar credenciales).

> El primer conjunto de credenciales que agregue a Astra Control siempre está en uso porque Astra Control utiliza las credenciales para autenticarse en el bloque de copia de seguridad. Lo mejor es no eliminar estas credenciales.

Pasos

1. Seleccione **cuenta > credenciales**.
2. Seleccione la lista desplegable de la columna **Estado** para las credenciales que desea quitar.
3. Seleccione **Quitar**.
4. Escriba el nombre de las credenciales que desea confirmar la eliminación y, a continuación, seleccione **Sí, Eliminar credenciales**.

Resultado

Astra Control elimina las credenciales de la cuenta.

Rotar credenciales

Puede rotar credenciales en su cuenta. Si gira las credenciales, gírelos durante una ventana de mantenimiento cuando no haya copias de seguridad en curso (programadas o bajo demanda).

Pasos

1. Elimine las credenciales existentes siguiendo los pasos de Quite las credenciales.
2. Añada las nuevas credenciales siguiendo los pasos del Añada credenciales.
3. Actualice todos los bloques para usar las credenciales nuevas:
   a. En la navegación de la izquierda, seleccione **Cuchos**.
   b. Seleccione la lista desplegable en la columna **acciones** para el segmento que desea editar.
   c. Seleccione **Editar**.
   d. En la sección **Seleccionar credenciales**, elija las nuevas credenciales que agregó a Astra Control.
   e. Seleccione **Actualizar**.
   f. Repita los pasos **b** a **e** para los cucharones restantes del sistema.

Resultado

Astra Control empieza a utilizar las nuevas credenciales del proveedor de cloud.

Controlar la actividad de la cuenta

Puede ver los detalles de las actividades en su cuenta de Astra Control. Por ejemplo, cuando se invitó a nuevos usuarios, cuando se agregaba un clúster o cuando se tomaba una snapshot. También puede exportar la actividad de su cuenta a un archivo CSV.

Ver toda la actividad de la cuenta en Astra Control

1. Seleccione **actividad**.
2. Utilice los filtros para restringir la lista de actividades o utilice el cuadro de búsqueda para encontrar exactamente lo que busca.
3. Seleccione **Exportar a CSV** para descargar la actividad de su cuenta en un archivo CSV.

Ver la actividad de la cuenta de una aplicación específica

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. Seleccione **actividad**.

Ver la actividad de la cuenta de los clústeres

1. Seleccione **Clusters** y, a continuación, seleccione el nombre del clúster.
2. Seleccione **actividad**.

Ver y gestionar notificaciones

Astra Control le avisa cuando las acciones se han completado o han fallado. Por ejemplo, verá una notificación si una copia de seguridad de una aplicación se ha completado correctamente.

El número de notificaciones sin leer está disponible en la parte superior derecha de la interfaz.

Puede ver estas notificaciones y marcarlas como leídas (esto puede ser útil si desea borrar notificaciones no leídas como nosotros).

Pasos

1. Seleccione el número de notificaciones sin leer en la parte superior derecha.
2. Revise las notificaciones y seleccione **Marcar como leído** o **Mostrar todas las notificaciones**.

   Si ha seleccionado **Mostrar todas las notificaciones**, se cargará la página Notificaciones.

3. En la página **Notificaciones**, vea las notificaciones, seleccione las que desea marcar como leídas, seleccione **Acción** y seleccione **Marcar como leído**.

Cierre la cuenta

Si ya no necesita su cuenta de Astra Control, puede cerrarla en cualquier momento.

> Los bloques creados automáticamente por Astra Control se eliminarán automáticamente al cerrar la cuenta.

Pasos

1. "Desgestione todas las aplicaciones y clústeres".
2. "Eliminar credenciales de Astra Control".
3. Seleccione **cuenta > facturación > método de pago**.
4. Seleccione **Cerrar cuenta**.
5. Introduzca el nombre de su cuenta y confirme que desea cerrar la cuenta.

Gestionar las instancias de cloud

Una instancia de cloud es un dominio único dentro de un proveedor de cloud. Es posible crear varias instancias de cloud para cada proveedor de cloud y cada instancia de cloud tiene su propio nombre, credenciales y clústeres asociados.

Cree una instancia de cloud cuando agregue un nuevo clúster a Astra Control. Puede editar una instancia de cloud para cambiar su nombre o bloque predeterminado mediante la interfaz de usuario de Astra Control y realizar otras acciones con la instancia de cloud mediante la API Astra Control.

Añadir una instancia de cloud

Puede añadir una nueva instancia de cloud cuando agregue un clúster nuevo a Astra Control. Consulte "Empiece a gestionar los clústeres de Kubernetes desde Astra Control Service" si quiere más información.

Editar una instancia de cloud

Puede modificar una instancia de cloud existente para un proveedor de cloud.

Pasos

1. Vaya a **instancias de cloud**.
2. En la lista de instancias de nube, seleccione el menú **acciones** para la instancia de nube que desee editar.
3. Seleccione **Editar**.

   En esta página, puede actualizar el nombre y el bloque predeterminado de la instancia de cloud.

   > Cada instancia de cloud de Astra Control debe tener un nombre único.

Gire las credenciales de una instancia de cloud

Puede utilizar la API Astra Control para rotar las credenciales de una instancia en la nube. Para obtener más información, "Vaya a los documentos de automatización de Astra".

Quitar una instancia de cloud

Puede usar la API Astra Control para eliminar una instancia de cloud de un proveedor de cloud. Para obtener

más información, "Vaya a los documentos de automatización de Astra".

Habilita el aprovisionador de Astra Control

Las versiones 23,10 y posteriores de Astra Trident incluyen la opción de usar Astra Control Provisioning, que permite a los usuarios de Astra Control con licencia acceder a funcionalidades avanzadas de aprovisionamiento del almacenamiento. El aprovisionador Astra Control ofrece esta funcionalidad ampliada, además de la funcionalidad estándar basada en CSI de Astra Trident. Puedes usar este procedimiento para habilitar e instalar el aprovisionador de Astra Control.

Tu suscripción al servicio de Astra Control incluye automáticamente la licencia para el uso del aprovisionador de Astra Control.

En las próximas actualizaciones de Astra Control, el aprovisionador de Astra Control reemplazará a Astra Trident como aprovisionador de almacenamiento y orquestador y será obligatorio para su uso en Astra Control. Por este motivo, se recomienda encarecidamente que los usuarios de Astra Control habiliten el aprovisionador de Astra Control. Astra Trident seguirá siendo de código abierto y se seguirá lanzando, manteniendo, admitiendo y actualizando con las nuevas funciones CSI y otras de NetApp.

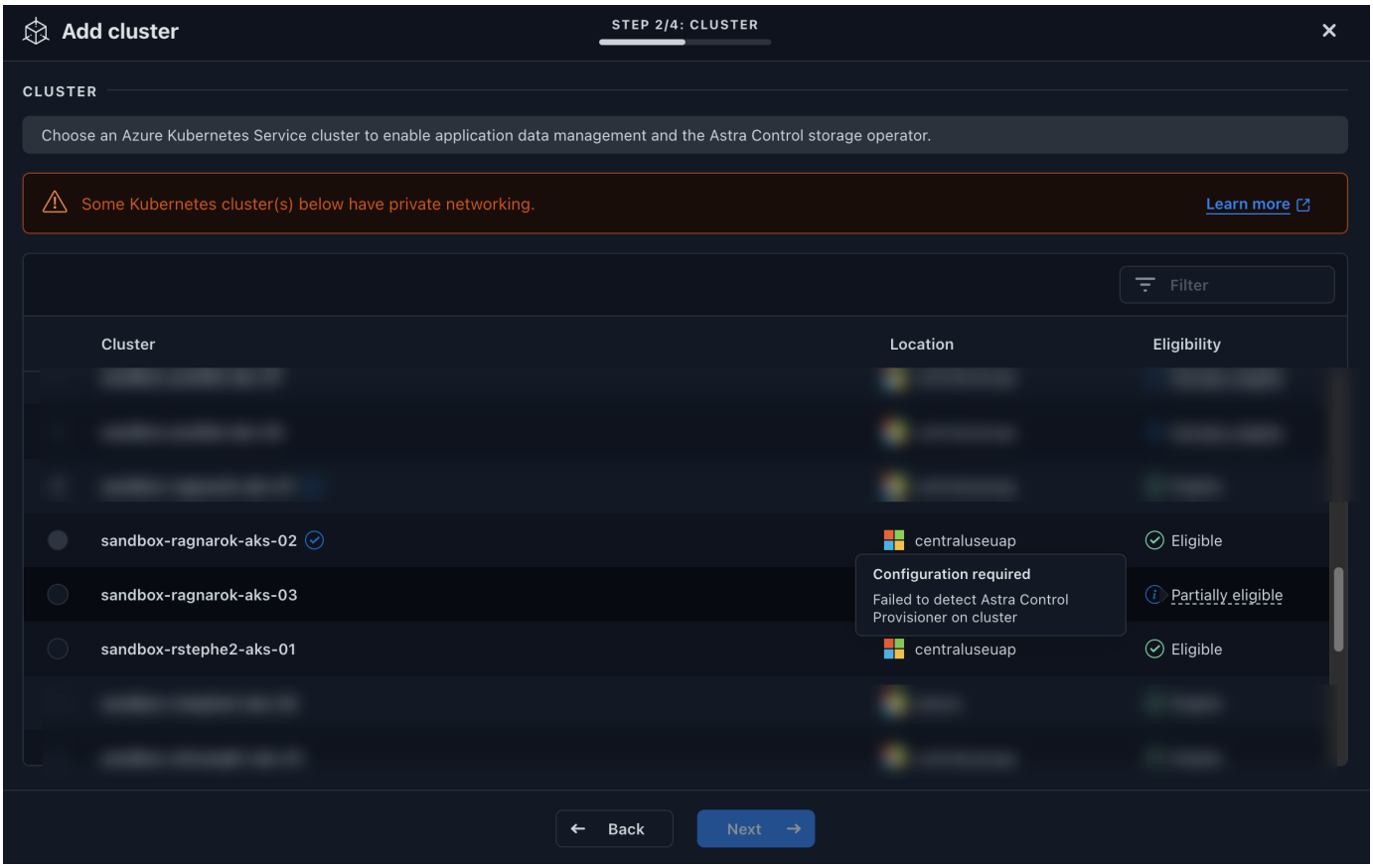
¿Cómo puedo saber si debo habilitar Astra Control Provisioner?

Si agrega un clúster a Astra Control Service que no tenga Astra Trident instalado previamente, el clúster se marcará como `Eligible`. Usted primero "Añada el clúster a Astra Control", Astra Control Provisioner se activará automáticamente.

Si el clúster no está marcado `Eligible`, se marcará `Partially eligible` debido a una de las siguientes razones:

- Está usando una versión anterior de Astra Trident
- Se utiliza un Astra Trident 23,10 que aún no tiene habilitada la opción de aprovisionador
- Se trata de un tipo de clúster que no permite la habilitación automática

Para `Partially eligible` Casos, usa estas instrucciones para habilitar manualmente el aprovisionador de Astra Control en tu clúster.



Antes de habilitar Astra Control Provisioner

Si ya tienes un Astra Trident sin el aprovisionador de Astra Control y quieres habilitar el aprovisionador de Astra Control, haz lo siguiente primero:

- **Si tienes Astra Trident instalado, confirma que su versión está dentro de una ventana de cuatro versiones**: Puedes realizar una actualización directa a Astra Trident 24,02 con el aprovisionador de control de Astra si tu Astra Trident está dentro de una ventana de cuatro versiones de la versión 24,02. Por ejemplo, puedes actualizar directamente de Astra Trident 23,04 a 24,02.
- **Confirme que su clúster tiene una arquitectura de sistema AMD64**: La imagen del aprovisionador de Astra Control se proporciona en las arquitecturas de CPU AMD64 y ARM64, pero solo AMD64 es compatible con Astra Control.

Pasos

1. Acceda al registro de imágenes de Astra Control de NetApp:
   a. Inicia sesión en la interfaz de usuario de Astra Control Service y registra tu ID de cuenta de Astra Control.
      i. Seleccione el icono de figura en la parte superior derecha de la página.
      ii. Seleccione **acceso API**.
      iii. Escriba su ID de cuenta.
   b. En la misma página, selecciona **Generar token de API** y copia la cadena de token de API en el portapapeles y guárdalo en tu editor.
   c. Inicia sesión en el registro de Astra Control usando el método que prefieras:

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

```
crane auth login cr.astra.netapp.io -u <account-id> -p <api-token>
```

2. (Solo registros personalizados) Siga estos pasos para mover la imagen a su registro personalizado. Si no está utilizando un registro, siga los pasos del operador Trident en la siguiente sección.

> Puede usar Podman en lugar de Docker para los siguientes comandos. Si se utiliza un entorno de Windows, se recomienda PowerShell.

Docker

a. Extrae la imagen del aprovisionador de Astra Control del registro:

> La imagen extraída no soportará múltiples plataformas y solo soportará la misma plataforma que el host que sacó la imagen, como Linux AMD64.

```
docker pull cr.astra.netapp.io/astra/trident-acp:24.02.0
--platform <cluster platform>
```

Ejemplo:

```
docker pull cr.astra.netapp.io/astra/trident-acp:24.02.0
--platform linux/amd64
```

b. Etiquete la imagen:

```
docker tag cr.astra.netapp.io/astra/trident-acp:24.02.0
<my_custom_registry>/trident-acp:24.02.0
```

c. Introduzca la imagen en el registro personalizado:

```
docker push <my_custom_registry>/trident-acp:24.02.0
```

Grúa

a. Copie el manifiesto de Astra Control Provisioner en su registro personalizado:

```
crane copy cr.astra.netapp.io/astra/trident-acp:24.02.0
<my_custom_registry>/trident-acp:24.02.0
```

3. Determinar si el método de instalación original de Astra Trident utilizó un.
4. Habilita el aprovisionamiento de Astra Control en Astra Trident con el método de instalación que solías originalmente:

Operador Astra Trident

a. "Descarga el instalador de Astra Trident y extráigalo".

b. Complete estos pasos si todavía no ha instalado Astra Trident o si ha quitado el operador de la implementación original de Astra Trident:

   i. Cree el CRD:

```
kubectl create -f
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.1
6.yaml
```

   ii. Cree el espacio de nombres trident (`kubectl create namespace trident`) o confirme que el espacio de nombres trident sigue existiendo (`kubectl get all -n trident`). Si el espacio de nombres se ha eliminado, vuelva a crearlo.

c. Actualice Astra Trident a 24.02.0:

> Para los clústeres que ejecutan Kubernetes 1,24 o una versión anterior, utilice `bundle_pre_1_25.yaml`. Para los clústeres que ejecutan Kubernetes 1,25 o posterior, utilice `bundle_post_1_25.yaml`.

```
kubectl -n trident apply -f trident-installer/deploy/<bundle-
name.yaml>
```

d. Compruebe que Astra Trident está ejecutando:

```
kubectl get torc -n trident
```

Respuesta:

```
NAME      AGE
trident   21m
```

e. Si tienes un registro que usa secretos, crea un secreto para extraer la imagen del aprovisionador de Astra Control:

```
kubectl create secret docker-registry <secret_name> -n trident
--docker-server=<my_custom_registry> --docker-username=<username>
--docker-password=<token>
```

f. Edite el CR de TridentOrchestrator y realice las siguientes modificaciones:

```
kubectl edit torc trident -n trident
```

i. Establezca una ubicación de registro personalizada para la imagen de Astra Trident o extráigala del registro de Astra Control (`tridentImage: <my_custom_registry>/trident:24.02.0` o. `tridentImage: netapp/trident:24.02.0`).

ii. Habilita el aprovisionador de Astra Control (`enableACP: true`).

iii. Establezca la ubicación de registro personalizada para la imagen del aprovisionador de Astra Control o sáquela del registro de Astra Control (`acpImage: <my_custom_registry>/trident-acp:24.02.0` o. `acpImage: cr.astra.netapp.io/astra/trident-acp:24.02.0`).

iv. Si estableció la imagen descubre los secretos anteriormente en este procedimiento, puede establecerlos aquí (`imagePullSecrets: - <secret_name>`). Utilice el mismo nombre secreto que estableció en los pasos anteriores.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  tridentImage: <registry>/trident:24.02.0
  enableACP: true
  acpImage: <registry>/trident-acp:24.02.0
  imagePullSecrets:
  - <secret_name>
```

g. Guarde y salga del archivo. El proceso de despliegue comenzará automáticamente.

h. Compruebe que se han creado el operador, el despliegue y los replicasets.

```
kubectl get all -n trident
```

> Solo debe haber **una instancia** del operador en un clúster de Kubernetes. No cree varias implementaciones del operador Trident de Astra.

i. Compruebe el `trident-acp` container se está ejecutando y eso `acpVersion` es `24.02.0` con el estado de `Installed`:

```
kubectl get torc -o yaml
```

Respuesta:

```
status:
  acpVersion: 24.02.0
  currentInstallationParams:
    ...
    acpImage: <registry>/trident-acp:24.02.0
    enableACP: "true"
    ...
  ...
  status: Installed
```

tridentctl

a. "Descarga el instalador de Astra Trident y extráigalo".

b. "Si ya tiene un Astra Trident existente, desinstálelo del clúster que lo aloja".

c. Instale Astra Trident con el aprovisionador de control de Astra habilitado (`--enable-acp=true`):

```
./tridentctl -n trident install --enable-acp=true --acp
-image=mycustomregistry/trident-acp:24.02
```

d. Confirme que se ha habilitado el aprovisionador de Astra Control:

```
./tridentctl -n trident version
```

Respuesta:

```
+----------------+----------------+-------------+ | SERVER
VERSION | CLIENT VERSION | ACP VERSION | +----------------
+----------------+-------------+ | 24.02.0 | 24.02.0 | 24.02.0. |
+----------------+----------------+-------------+
```

Timón

a. Si tiene Astra Trident 23.07.1 o anterior instalado, "desinstalar" el operador y otros componentes.

b. Si tu clúster de Kubernetes ejecuta la versión 1,24 o anterior, elimina psp:

```
kubectl delete psp tridentoperatorpod
```

c. Añada el repositorio de Astra Trident Helm:

```
helm repo add netapp-trident https://netapp.github.io/trident-
helm-chart
```

d. Actualice el gráfico Helm:

```
helm repo update netapp-trident
```

Respuesta:

```
Hang tight while we grab the latest from your chart
repositories...
...Successfully got an update from the "netapp-trident" chart
repository
Update Complete. ⎈Happy Helming!⎈
```

e. Enumere las imágenes:

```
./tridentctl images -n trident
```

Respuesta:

```
| v1.28.0            | netapp/trident:24.02.0|
|                    | docker.io/netapp/trident-
autosupport:24.02|
|                    | registry.k8s.io/sig-storage/csi-
provisioner:v4.0.0|
|                    | registry.k8s.io/sig-storage/csi-
attacher:v4.5.0|
|                    | registry.k8s.io/sig-storage/csi-
resizer:v1.9.3|
|                    | registry.k8s.io/sig-storage/csi-
snapshotter:v6.3.3|
|                    | registry.k8s.io/sig-storage/csi-node-
driver-registrar:v2.10.0 |
|                    | netapp/trident-operator:24.02.0 (optional)
```

f. Asegúrese de que el trident-operator 24.02.0 esté disponible:

```
helm search repo netapp-trident/trident-operator --versions
```

Respuesta:

```
NAME                            CHART VERSION   APP VERSION
DESCRIPTION
netapp-trident/trident-operator 100.2402.0      24.02.0         A
```

g. Uso `helm install` y ejecute una de las siguientes opciones que incluyen estos ajustes:
   - Un nombre para la ubicación de despliegue
   - La versión de Trident de Astra
   - El nombre de la imagen del aprovisionador de Astra Control
   - La marca para habilitar el aprovisionador
   - (Opcional) Una ruta de registro local. Si está utilizando un registro local, su "Imágenes de Trident" Se pueden ubicar en un registro o en diferentes registros, pero todas las imágenes CSI deben estar ubicadas en el mismo registro.
   - El espacio de nombres de Trident

Opciones

- Imágenes sin registro

```
helm install trident netapp-trident/trident-operator --version
100.2402.0 --set acpImage=cr.astra.netapp.io/astra/trident-
acp:24.02.0 --set enableACP=true --set operatorImage=netapp/trident-
operator:24.02.0 --set
tridentAutosupportImage=docker.io/netapp/trident-autosupport:24.02
--set tridentImage=netapp/trident:24.02.0 --namespace trident
```

- Imágenes en uno o más registros

```
helm install trident netapp-trident/trident-operator --version
100.2402.0 --set acpImage=<your-registry>:<acp image> --set
enableACP=true --set imageRegistry=<your-registry>/sig-storage --set
operatorImage=netapp/trident-operator:24.02.0 --set
tridentAutosupportImage=docker.io/netapp/trident-autosupport:24.02
--set tridentImage=netapp/trident:24.02.0 --namespace trident
```

Puede utilizar `helm list` para revisar detalles de la instalación como nombre, espacio de nombres, gráfico, estado, versión de la aplicación, y el número de revisión.

Si tiene problemas para poner en marcha Trident mediante Helm, ejecute este comando para desinstalar completamente Astra Trident:

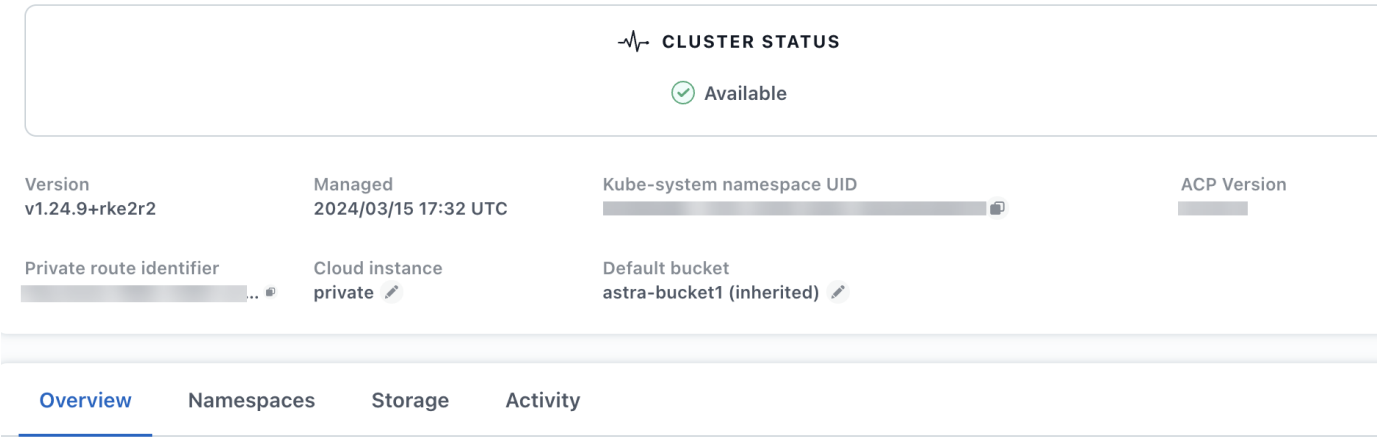
```
./tridentctl uninstall -n trident
```

No "Elimina por completo los CRD de Astra Trident" Como parte de la desinstalación antes de intentar habilitar de nuevo Astra Control Provisioner.

Resultado

Está habilitada la funcionalidad de aprovisionamiento de Astra Control y es posible usar cualquier función disponible para la versión que esté ejecutando.

Después de instalar el aprovisionador de Astra Control, el clúster que aloja el aprovisionador en la interfaz de usuario de Astra Control mostrará una `ACP version` en lugar de `Trident version` campo y núm. de versión instalada actual.



Si quiere más información

- "Documentación sobre actualizaciones de Astra Trident"

Desgestione aplicaciones y clústeres

Elimine las aplicaciones o clústeres que ya no desee gestionar desde Astra Control.

Deje de gestionar una aplicación

Detenga la gestión de las aplicaciones de las que ya no quiera realizar copias de seguridad, copias Snapshot o clones de Astra Control.

Al anular la gestión de una aplicación:

- Se eliminarán todos los backups y las snapshots existentes.
- Las aplicaciones y los datos siguen estando disponibles.

Pasos

1. En la barra de navegación izquierda, seleccione **aplicaciones**.
2. Seleccione la aplicación.
3. En el menú Opciones de la columna acciones, seleccione **Unmanage**.
4. Revise la información.
5. Escriba "desgestionar" para confirmar.

6. Seleccione **Sí, Desactivar aplicación**.

Resultado

Astra Control deja de gestionar la aplicación.

Deje de gestionar un clúster

Deje de gestionar el clúster que ya no desea gestionar desde Astra Control.

> Antes de anular la administración del clúster, debe anular la administración de las aplicaciones asociadas al clúster.

Como práctica recomendada, le recomendamos que quite el clúster de Astra Control antes de eliminarlo a través de GCP.

Cuando se desadministra un clúster:

- Esta acción evita que Astra Control gestione su clúster. No realiza cambios en la configuración del clúster y no elimina el clúster.
- El aprovisionador Astra Control o Astra Trident no se desinstalarán del clúster. "Descubra cómo desinstalar Astra Trident".

Pasos

1. Seleccione **Clusters**.
2. Seleccione la casilla de comprobación del clúster que ya no desea gestionar.
3. En el menú de opciones de la columna **Acciones**, selecciona **Desgestionar**.
4. Confirme que desea anular la gestión del clúster y, a continuación, seleccione **Sí, anular la gestión**.

Resultado

El estado del clúster cambia a **Extracción**. Después de eso, el clúster se eliminará de la página **Clusters** y Astra Control ya no lo gestionará.

Elimine clústeres de su proveedor de cloud

Antes de eliminar un clúster de Kubernetes que tiene volúmenes persistentes (VP) que residen en clases de almacenamiento de NetApp, primero debe eliminar las reclamaciones de volumen persistente (RVP) siguiendo uno de los métodos siguientes. Eliminar la RVP y el VP antes de eliminar el clúster garantiza que no recibirá facturas inesperadas del proveedor de cloud.

- **método #1**: Elimina los espacios de nombres de la carga de trabajo de la aplicación del clúster. *not* elimine el espacio de nombres Trident.
- **método #2**: Elimine las CVP y las vainas, o el despliegue donde se montan las Vs.

Cuando gestiona un clúster de Kubernetes desde Astra Control, las aplicaciones de ese clúster utilizan su proveedor de cloud como back-end de almacenamiento para volúmenes persistentes. Si elimina el clúster del proveedor de cloud sin eliminar primero los VP, los volúmenes back-end se *not* eliminan junto con el clúster.

Si utiliza uno de los métodos anteriores, se eliminarán los correspondientes VP de su clúster. Asegúrese de que no existan VP en las clases de almacenamiento de NetApp en el clúster antes de eliminarlo.

Si no eliminó los volúmenes persistentes antes de eliminar el clúster, deberá eliminar manualmente los

volúmenes de back-end del proveedor de cloud.

Pon en marcha una instancia autogestionada de Astra Control

Si deseas una instancia autogestionada de Astra Control que resida dentro de tu red, puedes poner en marcha Astra Control Center directamente desde Astra Control Service.

Pasos

1. En el área Primeros pasos del Dashboard, selecciona **Desplegar una instancia autogestionada de Astra Control**.
2. Debe realizar una de las siguientes acciones:
   - Genere un nuevo token de API seleccionando **Generar**.
   - Pegue en un token de API de REST DE Astra Control existente. Consulte la "Documentación de Astra Automation" Para obtener orientación sobre la generación de un token de API.
3. Sigue las instrucciones en la ventana **Implementar Astra Control Center**.

Use el aprovisionador de Astra Control

Configurar el cifrado de backend de almacenamiento

Con Astra Control Provisioning, puede mejorar la seguridad de acceso a los datos al habilitar el cifrado del tráfico entre su clúster gestionado y el back-end de almacenamiento.

Astra Control Provisioning admite el cifrado Kerberos para dos tipos de back-ends de almacenamiento:

- **ONTAP en las instalaciones** - El aprovisionador de control de Astra admite el cifrado de Kerberos a través de conexiones NFSv3 y NFSv4 desde Red Hat OpenShift y los clústeres de Kubernetes ascendentes a volúmenes ONTAP locales.
- **Azure NetApp Files** - El aprovisionador de control de Astra admite el cifrado de Kerberos a través de conexiones NFSv4,1 desde clústeres de Kubernetes anteriores a volúmenes de Azure NetApp Files.

Puede crear, eliminar, cambiar el tamaño, copiar, clonar, Clone de solo lectura e importe volúmenes que usen cifrado NFS.

Configure el cifrado de Kerberos en tránsito con volúmenes de ONTAP en las instalaciones

Puede habilitar el cifrado de Kerberos en el tráfico de almacenamiento entre su clúster gestionado y un back-end de almacenamiento de ONTAP en las instalaciones.

> El cifrado de Kerberos para el tráfico NFS con back-ends de almacenamiento de ONTAP en las instalaciones solo se admite mediante el `ontap-nas` controlador de almacenamiento.

Antes de empezar

- Asegúrese de que tiene "Habilitado Astra Control Provisioning" en el clúster gestionado.
- Asegúrese de tener acceso al `tridentctl` utilidad.
- Asegúrese de tener acceso de administrador al back-end de almacenamiento de ONTAP.
- Asegúrese de conocer el nombre del volumen o los volúmenes que compartirá desde el back-end de almacenamiento ONTAP.
- Asegúrese de haber preparado la máquina virtual de almacenamiento de ONTAP para admitir el cifrado de Kerberos para los volúmenes de NFS. Consulte "Habilite Kerberos en una LIF de datos" si desea obtener instrucciones.
- Asegúrese de que los volúmenes de NFSv4 GB que utilice con el cifrado de Kerberos se hayan configurado correctamente. Consulte la sección Configuración de dominio de NetApp NFSv4 (página 13) del "Guía de mejoras y prácticas recomendadas de NetApp NFSv4".

Añada o modifique las políticas de exportación de ONTAP

Tiene que agregar reglas a políticas de exportación de ONTAP existentes o crear nuevas políticas de exportación que sean compatibles con el cifrado de Kerberos para el volumen raíz de la máquina virtual de almacenamiento de ONTAP, así como para cualquier volumen de ONTAP compartido con el clúster de Kubernetes ascendente. Las reglas de políticas de exportación que añada, o las nuevas políticas de exportación que cree, deben admitir los siguientes protocolos de acceso y permisos de acceso:

Protocolos de acceso

Configure la directiva de exportación con los protocolos de acceso NFS, NFSv3 y NFSv4.

Detalles de acceso

Puede configurar una de tres versiones diferentes de cifrado de Kerberos, según las necesidades del volumen:

- **Kerberos 5** - (autenticación y cifrado)
- **Kerberos 5i** - (autenticación y encriptación con protección de identidad)
- **Kerberos 5p** - (autenticación y encriptación con protección de identidad y privacidad)

Configure la regla de política de exportación de ONTAP con los permisos de acceso adecuados. Por ejemplo, si los clústeres montarán los volúmenes NFS con una combinación de Kerberos 5i y cifrado Kerberos 5p, utilice los siguientes ajustes de acceso:

Tipo	Acceso de solo lectura	Acceso de lectura/escritura	Acceso de superusuario
UNIX	Activado	Activado	Activado
Kerberos 5i	Activado	Activado	Activado
Kerberos 5p	Activado	Activado	Activado

Consulte la siguiente documentación para saber cómo crear políticas de exportación de ONTAP y reglas de políticas de exportación:

- "Cree una política de exportación"
- "Añada una regla a una política de exportación"

Cree un back-end de almacenamiento

Puede crear una configuración de back-end de almacenamiento de Astra Control Provisioner que incluya la funcionalidad de cifrado Kerberos.

Acerca de esta tarea

Al crear un archivo de configuración de backend de almacenamiento que configure el cifrado Kerberos, puede especificar una de las tres versiones diferentes del cifrado Kerberos mediante el `spec.nfsMountOptions` parámetro:

- `spec.nfsMountOptions: sec=krb5` (autenticación y cifrado)
- `spec.nfsMountOptions: sec=krb5i` (autenticación y cifrado con protección de identidad)
- `spec.nfsMountOptions: sec=krb5p` (autenticación y encriptación con protección de identidad y privacidad)

Especifique solo un nivel de Kerberos. Si especifica más de un nivel de cifrado de Kerberos en la lista de parámetros, sólo se utilizará la primera opción.

Pasos

1. En el clúster gestionado, cree un archivo de configuración de back-end de almacenamiento utilizando el ejemplo siguiente. Sustituya los valores entre paréntesis <> por información de su entorno:

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: backend-ontap-nas-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-ontap-nas
spec:
  version: 1
  storageDriverName: "ontap-nas"
  managementLIF: <STORAGE_VM_MGMT_LIF_IP_ADDRESS>
  dataLIF: <PROTOCOL_LIF_FQDN_OR_IP_ADDRESS>
  svm: <STORAGE_VM_NAME>
  username: <STORAGE_VM_USERNAME_CREDENTIAL>
  password: <STORAGE_VM_PASSWORD_CREDENTIAL>
  nasType: nfs
  nfsMountOptions: ["sec=krb5i"] #can be krb5, krb5i, or krb5p
  qtreesPerFlexvol:
  credentials:
    name: backend-ontap-nas-secret
```

2. Utilice el archivo de configuración que creó en el paso anterior para crear el backend:

```
tridentctl create backend -f <backend-configuration-file>
```

Si la creación del back-end falla, algo está mal con la configuración del back-end. Puede ver los registros para determinar la causa ejecutando el siguiente comando:

```
tridentctl logs
```

Después de identificar y corregir el problema con el archivo de configuración, puede ejecutar de nuevo el comando create.

Cree una clase de almacenamiento

Puede crear una clase de almacenamiento para aprovisionar volúmenes con el cifrado de Kerberos.

Acerca de esta tarea

Al crear un objeto de clase de almacenamiento, puede especificar una de las tres versiones diferentes del cifrado de Kerberos mediante el `mountOptions` parámetro:

- `mountOptions: sec=krb5` (autenticación y cifrado)
- `mountOptions: sec=krb5i` (autenticación y cifrado con protección de identidad)
- `mountOptions: sec=krb5p` (autenticación y encriptación con protección de identidad y privacidad)

Especifique solo un nivel de Kerberos. Si especifica más de un nivel de cifrado de Kerberos en la lista de parámetros, sólo se utilizará la primera opción. Si el nivel de cifrado especificado en la configuración de backend de almacenamiento es diferente al nivel especificado en el objeto de clase de almacenamiento, el objeto de clase de almacenamiento tiene prioridad.

Pasos

1. Cree un objeto de Kubernetes StorageClass, mediante el siguiente ejemplo:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nas-sc
provisioner: csi.trident.netapp.io
mountOptions: ["sec=krb5i"] #can be krb5, krb5i, or krb5p
parameters:
  backendType: "ontap-nas"
  storagePools: "ontapnas_pool"
  trident.netapp.io/nasType: "nfs"
allowVolumeExpansion: True
```

2. Cree la clase de almacenamiento:

```
kubectl create -f sample-input/storage-class-ontap-nas-sc.yaml
```

3. Asegúrese de que se ha creado la clase de almacenamiento:

```
kubectl get sc ontap-nas-sc
```

   Debería ver una salida similar a la siguiente:

```
NAME            PROVISIONER             AGE
ontap-nas-sc    csi.trident.netapp.io   15h
```

Aprovisione los volúmenes

Después de crear un back-end de almacenamiento y una clase de almacenamiento, ahora puede aprovisionar

un volumen. Consulte estas instrucciones para "aprovisionamiento de un volumen".

Configure el cifrado de Kerberos en tránsito con volúmenes Azure NetApp Files

Puede habilitar el cifrado de Kerberos en el tráfico de almacenamiento entre su clúster gestionado y un solo back-end de almacenamiento de Azure NetApp Files o un pool virtual de back-ends de almacenamiento de Azure NetApp Files.

Antes de empezar

- Asegúrese de haber habilitado el aprovisionador de Astra Control en el clúster Red Hat OpenShift gestionado. Consulte "Habilita el aprovisionador de Astra Control" si desea obtener instrucciones.
- Asegúrese de tener acceso al `tridentctl` utilidad.
- Asegúrese de haber preparado el back-end de almacenamiento de Azure NetApp Files para cifrado Kerberos siguiendo los requisitos y siguiendo las instrucciones de "Documentación de Azure NetApp Files".
- Asegúrese de que los volúmenes de NFSv4 GB que utilice con el cifrado de Kerberos se hayan configurado correctamente. Consulte la sección Configuración de dominio de NetApp NFSv4 (página 13) del "Guía de mejoras y prácticas recomendadas de NetApp NFSv4".

Cree un back-end de almacenamiento

Puede crear una configuración de back-end de almacenamiento de Azure NetApp Files que incluya la funcionalidad de cifrado de Kerberos.

Acerca de esta tarea

Cuando crea un archivo de configuración de backend de almacenamiento que configura el cifrado Kerberos, puede definirlo para que se aplique en uno de los dos niveles posibles:

- El **storage backend level** usando el `spec.kerberos` campo
- El **nivel de grupo virtual** usando el `spec.storage.kerberos` campo

Cuando se define la configuración en el nivel del pool virtual, el pool se selecciona con la etiqueta de la clase de almacenamiento.

En cualquier nivel, puede especificar una de las tres versiones diferentes del cifrado Kerberos:

- `kerberos: sec=krb5` (autenticación y cifrado)
- `kerberos: sec=krb5i` (autenticación y cifrado con protección de identidad)
- `kerberos: sec=krb5p` (autenticación y encriptación con protección de identidad y privacidad)

Pasos

1. En el clúster gestionado, cree un archivo de configuración de back-end de almacenamiento mediante uno de los siguientes ejemplos, en función del lugar donde necesite definir el back-end de almacenamiento (nivel de back-end de almacenamiento o nivel de pool virtual). Sustituya los valores entre paréntesis <> por información de su entorno:

Ejemplo de nivel de back-end de almacenamiento

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-anf-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-anf-secret
```

Ejemplo de nivel de pool virtual

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-anf-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  storage:
    - labels:
        type: encryption
      kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-anf-secret
```

2. Utilice el archivo de configuración que creó en el paso anterior para crear el backend:

```
tridentctl create backend -f <backend-configuration-file>
```

Si la creación del back-end falla, algo está mal con la configuración del back-end. Puede ver los registros para determinar la causa ejecutando el siguiente comando:

```
tridentctl logs
```

Después de identificar y corregir el problema con el archivo de configuración, puede ejecutar de nuevo el comando create.

Cree una clase de almacenamiento

Puede crear una clase de almacenamiento para aprovisionar volúmenes con el cifrado de Kerberos.

Pasos

1. Cree un objeto de Kubernetes StorageClass, mediante el siguiente ejemplo:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: anf-sc-nfs
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "nfs"
  selector: "type=encryption"
```

2. Cree la clase de almacenamiento:

```
kubectl create -f sample-input/storage-class-anf-sc-nfs.yaml
```

3. Asegúrese de que se ha creado la clase de almacenamiento:

```
kubectl get sc anf-sc-nfs
```

Debería ver una salida similar a la siguiente:

```
NAME          PROVISIONER              AGE
anf-sc-nfs     csi.trident.netapp.io   15h
```

Aprovisione los volúmenes

Después de crear un back-end de almacenamiento y una clase de almacenamiento, ahora puede aprovisionar un volumen. Consulte estas instrucciones para "aprovisionamiento de un volumen".

Recuperar datos de volumen mediante una copia Snapshot

Astra Control Provisioning permite restaurar volúmenes rápidamente sin movimiento a partir de una copia Snapshot mediante el `TridentActionSnapshotRestore` (TASR) CR. Esta CR funciona como una acción imprescindible de Kubernetes y no persiste una

vez que finaliza la operación.

Astra Control Provisioner admite la restauración de copias Snapshot en el `ontap-san`, `ontap-san-economy`, `ontap-nas`, `ontap-nas-flexgroup`, `azure-netapp-files`, `gcp-cvs`, y. `solidfire-san` de windows

Antes de empezar

Debe tener una snapshot de volumen disponible y la RVP vinculada.

- Compruebe que el estado de la RVP es de enlace.

```
kubectl get pvc
```

- Compruebe que la copia de Snapshot de volumen esté lista para utilizarse.

```
kubectl get vs
```

Pasos

1. Cree el CR de TASR. En este ejemplo se crea una CR para la RVP `pvc1` y copia de snapshot de volumen `pvc1-snapshot`.

```
cat tasr-pvc1-snapshot.yaml

apiVersion: v1
kind: TridentActionSnapshotRestore
metadata:
  name: this-doesnt-matter
  namespace: trident
spec:
  pvcName: pvc1
  volumeSnapshotName: pvc1-snapshot
```

2. Aplique el CR para restaurar a partir de la instantánea. En este ejemplo se restaura a partir de una copia Snapshot `pvc1`.

```
kubectl create -f tasr-pvc1-snapshot.yaml

tridentactionsnapshotrestore.trident.netapp.io/this-doesnt-matter
created
```

Resultados

El aprovisionador de Astra Control restaura los datos a partir de la snapshot. Es posible verificar el estado de restauración de la Snapshot.

```
kubectl get tasr -o yaml

apiVersion: v1
items:
- apiVersion: trident.netapp.io/v1
  kind: TridentActionSnapshotRestore
  metadata:
    creationTimestamp: "2023-04-14T00:20:33Z"
    generation: 3
    name: this-doesnt-matter
    namespace: trident
    resourceVersion: "3453847"
    uid: <uid>
  spec:
    pvcName: pvc1
    volumeSnapshotName: pvc1-snapshot
  status:
    startTime: "2023-04-14T00:20:34Z"
    completionTime: "2023-04-14T00:20:37Z"
    state: Succeeded
kind: List
metadata:
  resourceVersion: ""
```

- En la mayoría de los casos, el aprovisionador de Astra Control no volverá a intentar automáticamente la operación en caso de fallo. Deberá realizar la operación de nuevo.
- Es posible que el administrador deba conceder permiso al usuario de Kubernetes sin acceso de administrador para crear una CR TASR en su espacio de nombres de la aplicación.

Replicar volúmenes mediante SnapMirror

Con Astra Control Provisioning, puede crear relaciones de mirroring entre un volumen de origen en un clúster y el volumen de destino en el clúster con relación de paridad para replicar datos para la recuperación de desastres. Puede utilizar una definición de recursos personalizados (CRD) con nombre para realizar las siguientes operaciones:

- Crear relaciones de mirroring entre volúmenes (RVP)
- Elimine las relaciones de reflejo entre volúmenes
- Rompa las relaciones de reflejo
- Promocionar el volumen secundario durante condiciones de desastre (conmutaciones al respaldo).
- Realice una transición de las aplicaciones sin pérdidas de un clúster a otro (durante las migraciones y las conmutaciones al respaldo planificadas).

Requisitos previos de replicación

Asegúrese de que se cumplen los siguientes requisitos previos antes de comenzar:

Clústeres ONTAP

- **Astra Control Provisionador**: Astra Control Provisionador versión 23,10 o posterior debe existir en los clústeres de Kubernetes de origen y destino que utilizan ONTAP como backend.
- **Licencias**: Las licencias asíncronas de SnapMirror de ONTAP que utilizan el paquete de protección de datos deben estar habilitadas en los clústeres de ONTAP de origen y de destino. Consulte "Información general sobre las licencias de SnapMirror en ONTAP" si quiere más información.

Interconexión

- **Cluster y SVM**: Los back-ends de almacenamiento ONTAP deben ser peered. Consulte "Información general sobre relaciones entre iguales de clústeres y SVM" si quiere más información.

  > Compruebe que los nombres de las SVM utilizados en la relación de replicación entre dos clústeres de ONTAP sean únicos.

- **Astra Control Provisionador y SVM**: Las SVM remotas entre iguales deben estar disponibles para Astra Control Provisionador en el clúster de destino.

Controladores compatibles

- La replicación de volúmenes es compatible con los controladores ontap-nas y ontap-san.

Cree una RVP reflejada

Siga estos pasos y utilice los ejemplos de CRD para crear una relación de reflejo entre los volúmenes primario y secundario.

Pasos

1. Realice los siguientes pasos en el clúster de Kubernetes principal:
   a. Cree un objeto StorageClass con `trident.netapp.io/replication: true` parámetro.

      Ejemplo

      ```
      apiVersion: storage.k8s.io/v1
      kind: StorageClass
      metadata:
        name: csi-nas
      provisioner: csi.trident.netapp.io
      parameters:
        backendType: "ontap-nas"
        fsType: "nfs"
        trident.netapp.io/replication: "true"
      ```

   b. Cree una RVP con el tipo de almacenamiento creado anteriormente.

Ejemplo

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: csi-nas
spec:
  accessModes:
  - ReadWriteMany
  resources:
    requests:
      storage: 1Gi
  storageClassName: csi-nas
```

c. Cree un CR de MirrorRelationship con información local.

Ejemplo

```
kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
spec:
  state: promoted
  volumeMappings:
  - localPVCName: csi-nas
```

Astra Control Provisioner obtiene la información interna del volumen y el estado actual de protección de datos (DP) del volumen y, a continuación, rellena el campo de estado del MirrorRelationship.

d. Obtenga el TridentMirrorRelationship CR para obtener el nombre interno y SVM de la PVC.

```
kubectl get tmr csi-nas
```

```
kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
  generation: 1
spec:
  state: promoted
  volumeMappings:
  - localPVCName: csi-nas
status:
  conditions:
  - state: promoted
    localVolumeHandle:
"datavserver:trident_pvc_3bedd23c_46a8_4384_b12b_3c38b313c1e1"
    localPVCName: csi-nas
    observedGeneration: 1
```

2. Realice los siguientes pasos en el clúster de Kubernetes secundario:
   a. Cree una StorageClass con el parámetro trident.netapp.io/replication: true.

      Ejemplo

      ```
      apiVersion: storage.k8s.io/v1
      kind: StorageClass
      metadata:
        name: csi-nas
      provisioner: csi.trident.netapp.io
      parameters:
        trident.netapp.io/replication: true
      ```

   b. Cree un CR de MirrorRelationship con información de destino y origen.

      Ejemplo

      ```
      kind: TridentMirrorRelationship
      apiVersion: trident.netapp.io/v1
      metadata:
        name: csi-nas
      spec:
        state: established
        volumeMappings:
        - localPVCName: csi-nas
          remoteVolumeHandle:
      "datavserver:trident_pvc_3bedd23c_46a8_4384_b12b_3c38b313c1e1"
      ```

El aprovisionador de control de Astra creará una relación de SnapMirror con el nombre de la política de relaciones configurada (o predeterminado para ONTAP) e inicializarla.

c. Crear una RVP con StorageClass creado anteriormente para que actúe como secundario (destino de SnapMirror).

Ejemplo

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: csi-nas
  annotations:
    trident.netapp.io/mirrorRelationship: csi-nas
spec:
  accessModes:
  - ReadWriteMany
resources:
  requests:
    storage: 1Gi
storageClassName: csi-nas
```

El aprovisionador de control de Astra comprobará el CRD de TridentMirrorRelationship y no podrá crear el volumen si la relación no existe. Si existe la relación, el aprovisionador de Astra Control se asegurará de que el nuevo volumen de FlexVol se coloque en una SVM vinculada con la SVM remota definida en MirrorRelationship.

Estados de replicación de volúmenes

Una relación de mirroring de Trident (TMR) es un CRD que representa un extremo de una relación de replicación entre RVP. El TMR de destino tiene un estado, que le dice a Astra Control Provisioner cuál es el estado deseado. El TMR de destino tiene los siguientes estados:

- **Establecido**: El PVC local es el volumen de destino de una relación de espejo, y esta es una nueva relación.
- **Promocionado**: El PVC local es ReadWrite y montable, sin relación de espejo actualmente en vigor.
- **Reestablecido**: El PVC local es el volumen de destino de una relación de espejo y también estaba anteriormente en esa relación de espejo.
  - El estado reestablecido se debe usar si el volumen de destino alguna vez mantuvo una relación con el volumen de origen debido a que sobrescribe el contenido del volumen de destino.
  - El estado reestablecido generará un error si el volumen no mantuvo una relación anteriormente con el origen.

Promocione la RVP secundaria durante una conmutación al respaldo no planificada

Realice el siguiente paso en el clúster de Kubernetes secundario:

- Actualice el campo *spec.state* de TridentMirrorRelationship a. `promoted`.

Promocione la RVP secundaria durante una conmutación al respaldo planificada

Durante una conmutación al respaldo planificada (migración), realice los siguientes pasos para promocionar la RVP secundaria:

Pasos

1. En el clúster de Kubernetes principal, cree una snapshot de la RVP y espere hasta que se cree la snapshot.
2. En el clúster de Kubernetes principal, cree SnapshotInfo CR para obtener información interna.

   Ejemplo

   ```
   kind: SnapshotInfo
   apiVersion: trident.netapp.io/v1
   metadata:
     name: csi-nas
   spec:
     snapshot-name: csi-nas-snapshot
   ```

3. En el clúster de Kubernetes secundario, actualice el campo *spec.state* de *TridentMirrorRelationship* CR a *promoted* y *spec.promotedSnapshotHandle* para que sea InternalName de la snapshot.
4. En un clúster de Kubernetes secundario, confirme el estado (campo status.state) de TridentMirrorRelationship a Promoted.

Restaure una relación de mirroring después de una conmutación al nodo de respaldo

Antes de restaurar una relación de reflejo, elija el lado que desea realizar como el nuevo primario.

Pasos

1. En el clúster de Kubernetes secundario, compruebe que se actualicen los valores del campo *spec.remoteVolumeHandle* del TridentMirrorRelationship.
2. En el clúster de Kubernetes secundario, actualice el campo *spec.mirror* de TridentMirrorRelationship a `reestablished`.

Operaciones adicionales

Astra Control Provisioning admite las siguientes operaciones en los volúmenes primarios y secundarios:

Replica la PVC primaria a una nueva PVC secundaria

Asegúrese de que ya tiene un PVC primario y un PVC secundario.

Pasos

1. Elimine los CRD de PersistentVolumeClaim y TridentMirrorRelationship del clúster secundario (destino) establecido.
2. Elimine el CRD de TridentMirrorRelationship del clúster primario (origen).

3. Cree un nuevo CRD de TridentMirrorRelationship en el clúster primario (de origen) para la nueva PVC secundaria (de destino) que desea establecer.

Cambie el tamaño de una RVP reflejada, primaria o secundaria

El PVC se puede cambiar de tamaño como normal, ONTAP expandirá automáticamente cualquier flevxols de destino si la cantidad de datos excede el tamaño actual.

Elimine la replicación de una RVP

Para eliminar la replicación, realice una de las siguientes operaciones en el volumen secundario actual:

- Elimine el MirrorRelationship en la RVP secundaria. Esto interrumpe la relación de replicación.
- O bien, actualice el campo spec.state a *Promoted*.

Eliminar una RVP (que se había duplicado previamente)

Astra Control Provisioning comprueba si existen las RVP replicadas y libera la relación de replicación antes de intentar eliminar el volumen.

Eliminar un TMR

Al eliminar un TMR en un lado de una relación reflejada, el TMR restante pasará al estado *Promoted* antes de que Astra Control Provisioner complete la eliminación. Si el TMR seleccionado para eliminación ya se encuentra en el estado *Promoted*, no existe ninguna relación de reflejo y el TMR se eliminará y el aprovisionador de Astra Control promoverá la RVP local a *ReadWrite*. Esta eliminación libera los metadatos de SnapMirror del volumen local en ONTAP. Si este volumen se utiliza en una relación de reflejo en el futuro, debe utilizar un nuevo TMR con un estado de replicación de volumen *established* al crear la nueva relación de reflejo.

Actualice las relaciones de reflejo cuando el ONTAP esté en línea

Las relaciones de reflejos se pueden actualizar en cualquier momento una vez establecidas. Puede utilizar el `state: promoted` o. `state: reestablished` campos para actualizar las relaciones.
Al promocionar un volumen de destino a un volumen de ReadWrite normal, se puede usar *promotedSnapshotHandle* para especificar una snapshot específica a la que restaurar el volumen actual.

Actualice las relaciones de reflejo cuando la ONTAP esté sin conexión

Puede utilizar un CRD para realizar una actualización de SnapMirror sin Astra Control para tener conectividad directa con el clúster de ONTAP. Consulte el siguiente formato de ejemplo de TridentActionMirrorUpdate:

Ejemplo

```
apiVersion: trident.netapp.io/v1
kind: TridentActionMirrorUpdate
metadata:
  name: update-mirror-b
spec:
  snapshotHandle: "pvc-1234/snapshot-1234"
  tridentMirrorRelationshipName: mirror-b
```

`status.state` Refleja el estado del CRD TridentActionMirrorUpdate. Puede tomar un valor de *succeeded*, *in progress* o *failed*.

Automatización mediante la API REST de Astra Control

Astra Control dispone de una API REST que le permite acceder directamente a la funcionalidad Astra Control mediante un lenguaje de programación o una utilidad como Curl. También puede gestionar las puestas en marcha de Astra Control con Ansible y otras tecnologías de automatización.

Para obtener más información, "Vaya a los documentos de automatización de Astra".

Conocimiento y apoyo

Regístrese para recibir soporte

Astra Control intenta registrar automáticamente su cuenta para recibir asistencia cuando configura su cuenta. Si no puede, puede registrarse manualmente para recibir soporte usted mismo. Se requiere registro de soporte para obtener ayuda del soporte técnico de NetApp.

Compruebe el registro de soporte

Astra Control incluye un campo de estado de soporte que le permite confirmar su registro de soporte.

Pasos

1. Seleccione **Soporte**.
2. Eche un vistazo al campo Estado de soporte.

   El estado de soporte se iniciará como "no registrado", pero pasará a "en curso" y finalmente a "registrado" una vez completado.

   Este estado de registro de asistencia se registra cada 15 minutos. Los nuevos clientes de NetApp podrían tardar hasta el siguiente día laborable para completar la incorporación y el registro de soporte. Si el número de serie no muestra "registrado" en un plazo de 48 horas, puede ponerse en contacto con NetApp a través de astra.feedback@netapp.com o registrarse manualmente desde https://register.netapp.com.

Obtenga su número de serie

Al registrarse para obtener una cuenta, Astra Control utiliza la información que ha proporcionado sobre su empresa para generar un número de serie de 20 dígitos de NetApp que comienza con "941".

El número de serie de NetApp representa su cuenta de Astra Control. Deberá utilizar este número de serie al abrir una incidencia Web.

Puede encontrar el número de serie en la interfaz Astra Control en la página **Support**.

Active los derechos de soporte

Si Astra Control no pudo registrar automáticamente su cuenta para recibir soporte, debe registrar el número de serie de NetApp asociado a Astra Control para activar las autorizaciones de soporte. Ofrecemos 2 opciones de registro de soporte:

1. Cliente actual de NetApp con cuenta SSO existente del sitio de soporte de NetApp (NSS)
2. Nuevo cliente de NetApp sin cuenta SSO existente del sitio de soporte de NetApp (NSS)

Opción 1: Cliente actual de NetApp con una cuenta del sitio de soporte de NetApp (NSS) existente

Pasos

1. Desplácese hasta la "Registro de soporte de servicios de datos en el cloud" página.
2. Seleccione **ya estoy registrado como cliente de NetApp**.

3. Introduzca sus credenciales del sitio de soporte de NetApp para iniciar sesión.

   Aparece la página Registro de cliente existente.

4. Rellene la información necesaria en el formulario:
   a. Introduzca su nombre, empresa y dirección de correo electrónico.
   b. Selecciona **Astra Control Service** como línea de productos.
   c. Seleccione un proveedor de facturación.
   d. Escriba su número de serie.
   e. Seleccione **Enviar**.

Resultado

Debe ser redirigido a una página "Registro enviado correctamente". La dirección de correo electrónico asociada a su registro recibirá un mensaje de correo electrónico en un plazo de unos minutos que indica que "su producto ahora es elegible para recibir asistencia".

Este es un registro de soporte único para el número de serie aplicable.

Opción 2: Nuevo cliente de NetApp sin cuenta del sitio de soporte de NetApp (NSS)

Pasos

1. Desplácese hasta la "Registro de soporte de servicios de datos en el cloud" página.
2. Seleccione **no soy un cliente registrado de NetApp**.

   Aparecerá la página Registro de cliente nuevo.

3. Rellene la información necesaria en el formulario:
   a. Introduzca su nombre, información de la empresa y datos de contacto.
   b. Selecciona **Astra Control Service** como línea de productos.
   c. Seleccione un proveedor de facturación.
   d. Escriba su número de serie.
   e. Introduzca el valor captcha.
   f. Seleccione la casilla de verificación para confirmar que ha leído la Política de privacidad de NetApp.
   g. Seleccione **Enviar**.

      Recibirá un correo electrónico de confirmación de su registro enviado. Si no se produce ningún error, se le redirigirá a una página "Registro enviado correctamente". También recibirá un correo electrónico en un plazo de una hora que indica que "su producto es ahora elegible para recibir asistencia".

   Este es un registro de soporte único para el número de serie aplicable.

4. Como nuevo cliente de NetApp, también debe crear una cuenta de usuario del sitio de soporte de NetApp (NSS) para futuras activaciones de soporte, y para acceder al portal de soporte para chat de soporte técnico y elaboración de tickets web.

   Vaya a la "Sitio de registro de soporte de NetApp" para realizar esta tarea. Puede proporcionar el número de serie de Astra Control que acaba de registrar para acelerar el proceso.

Resolución de problemas

Aprenda a solucionar algunos problemas comunes que puede encontrar.

https://kb.netapp.com/Cloud/Astra/Control

Si quiere más información

- "Resolución de problemas"

Obtenga ayuda

NetApp ofrece compatibilidad con Astra Control de varias formas. Hay disponibles amplias opciones de soporte gratuito las 24 horas del día, los 7 días de la semana, como artículos de la base de conocimiento (KB) y un canal Discord. Su cuenta de Astra Control incluye soporte técnico remoto mediante emisión de boletos web.

Usted debe primero "Active el soporte para su número de serie de NetApp" para poder utilizar estas opciones de soporte no autoservicio. Se necesita una cuenta de SSO del sitio de soporte de NetApp (NSS) para el chat y los efectos de la emisión de boletos web junto con la gestión de casos.

Puede acceder a las opciones de soporte desde la interfaz de usuario de Astra Control seleccionando la pestaña **Soporte** del menú principal.

Autoasistencia

Estas opciones están disponibles de forma gratuita los siete días de la semana, las 24 horas

- "Base de conocimientos"

  Buscar artículos, preguntas frecuentes o información de reparaciones relacionadas con Astra Control.

- Documentación

  Este es el sitio de documentación que está viendo actualmente.

- "Obtenga ayuda con Discord"

  Vaya a Astra en la categoría Pub para ponerse en contacto con colegas y expertos.

- Correo electrónico de comentarios

  Envíe un correo electrónico a astra.feedback@netapp.com para informarnos de sus pensamientos, ideas o preocupaciones.

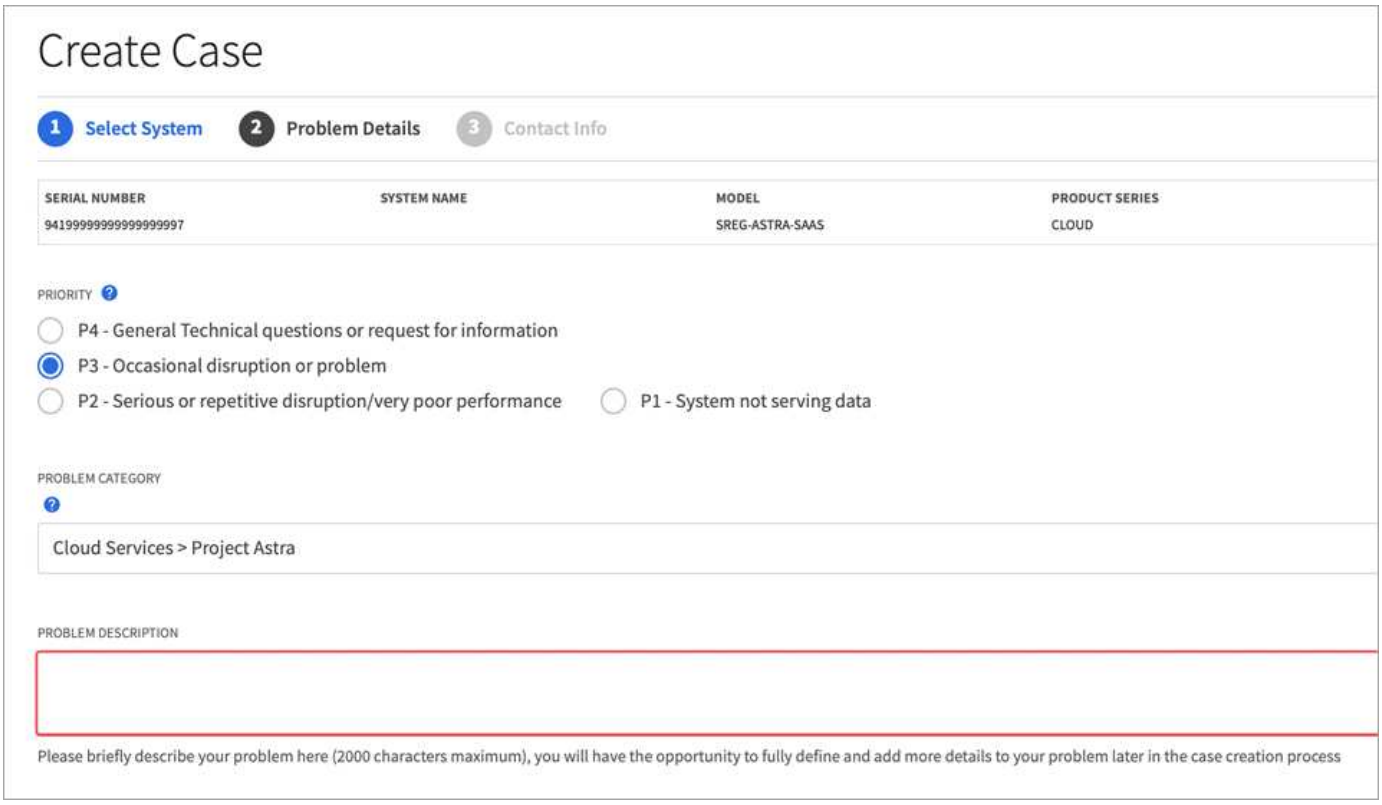
Soporte de suscripción

Además de las opciones de autosoporte anteriores, puede trabajar con un ingeniero de soporte de NetApp para resolver los problemas después de usted "Active el soporte para su número de serie de NetApp".

Una vez activado su número de serie de Astra Control, puede acceder a los recursos de soporte técnico de NetApp mediante la creación de una "Ticket de soporte".

Seleccione **Servicios de datos en la nube > Astra**.

Utilice el número de serie "941" para abrir el billete web. "Obtenga más información acerca de su número de serie".



Preguntas frecuentes

Estas preguntas frecuentes pueden ser de ayuda si solo está buscando una respuesta rápida a una pregunta.

Descripción general

Astra Control tiene como objetivo simplificar las operaciones de gestión del ciclo de vida de los datos de aplicaciones para aplicaciones nativas de Kubernetes. Astra Control Service admite clústeres de Kubernetes que se ejecutan en varios entornos de proveedores de cloud.

En las siguientes secciones se proporcionan respuestas a algunas preguntas adicionales que se pueden encontrar a medida que se utiliza Astra Control. Para obtener más aclaraciones, diríjase a astra.feedback@netapp.com

Acceso a Astra Control

¿Por qué tengo que proporcionar tantos detalles al registrarme en Astra Control?

Astra Control requiere información precisa del cliente al registrarse. Esta información es necesaria para pasar por una comprobación de Global Trade Compliance (GTC).

¿Por qué recibo un error de «Error de registro» al registrarme en Astra Control?

Astra Control requiere que proporcione información precisa sobre el cliente en la sección de incorporación. Obtendrá un error de "error de registro" si ha proporcionado información incorrecta. Otras cuentas de las que usted es miembro también se bloquean.

¿Qué es la URL del servicio de Astra Control?

Puede acceder al servicio Astra Control en https://astra.netapp.io.

He enviado una invitación por correo electrónico a un colega, pero no la han recibido. ¿Qué debo hacer?

Pídales que compruebe su carpeta de correo no deseado en busca de un correo electrónico en do-not-reply@netapp.com o busque "invitación" en su bandeja de entrada. También puede eliminar el usuario e intentar volver a agregarlos.

Me ascendí al Plan Premium PAYGO desde el Plan Gratuito. ¿Me cobrarán los primeros 10 espacios de nombres?

Sí. Después de actualizar al plan Premium, Astra Control empieza a cobrarle por todos los espacios de nombres gestionados de su cuenta.

Me ascendí al plan Premium PAYGO a mediados de un mes. ¿Me cobrarán todo el mes?

No La facturación comienza desde el momento en que se actualizó al plan Premium.

Estoy usando el plan gratuito, ¿se me cobrarán las reclamaciones de volumen persistente?

Sí, se le cobrará por los volúmenes persistentes que utilizan los clústeres de su proveedor de cloud.

Registrar clústeres de Kubernetes

¿Necesito instalar los controladores CSI en mi clúster antes de añadirlos a Astra Control Service?

No Cuando se añade el clúster a Astra Control, el servicio instalará automáticamente el controlador Astra Trident Container Storage Interface (CSI) en el clúster de Kubernetes. Este controlador CSI se utiliza para

aprovisionar volúmenes persistentes para clústeres respaldados por su proveedor de cloud.

Necesito agregar nodos de trabajador a mi clúster después de agregar a Astra Control Service. ¿Qué debo hacer?

Los nodos de trabajo nuevos se pueden añadir a los pools existentes o se pueden crear pools nuevos siempre que sean `COS_CONTAINERD` tipo de imagen. Estos serán descubiertos automáticamente por Astra Control. Si los nuevos nodos no están visibles en Astra Control, compruebe si los nuevos nodos de trabajo están ejecutando el tipo de imagen admitido. También puede verificar el estado de los nuevos nodos de trabajo mediante el `kubectl get nodes` comando.

Registrar clústeres de Elastic Kubernetes Service (EKS)

¿Puedo añadir un clúster de EKS privado a Astra Control Service?

Sí, puedes añadir clústeres de EKS privados a Astra Control Service. Para agregar un cluster EKS privado, consulte "Empiece a gestionar los clústeres de Kubernetes desde Astra Control Service".

Registrar clústeres de Azure Kubernetes Service (AKS)

¿Puedo añadir un clúster de AKS privado a Astra Control Service?

Sí, puede agregar clústeres AKS privados a Astra Control Service. Para agregar un clúster de AKS privado, consulte "Empiece a gestionar los clústeres de Kubernetes desde Astra Control Service".

¿Puedo usar Active Directory para administrar la autenticación de mis clústeres de AKS?

Sí, puede configurar sus clústeres AKS para usar Azure Active Directory (Azure AD) para la autenticación y la gestión de identidades. Cuando cree el clúster, siga las instrucciones que se indican en "documentación oficial" Para configurar el clúster de modo que use Azure AD. Debe asegurarse de que sus clústeres cumplen los requisitos de la integración de Azure AD gestionada por AKS.

Registrar clústeres de Google Kubernetes Engine (GKE)

¿Puedo agregar un clúster de GKE privado a Astra Control Service?

Sí, puede añadir clústeres GKE privados al servicio Astra Control. Para agregar un grupo de GKE privado, consulte "Empiece a gestionar los clústeres de Kubernetes desde Astra Control Service".

Los grupos de GKE privados deben tener el "redes autorizadas" Establezca esta opción para permitir la dirección IP de Astra Control:

52.188.218.166/32

¿Puede mi clúster de GKE residir en una VPC compartida?

Sí. Astra Control puede gestionar clústeres que residen en una VPC compartida. "Aprenda a configurar la cuenta de servicio Astra para una configuración VPC compartida".

¿Dónde puedo encontrar las credenciales de mi cuenta de servicio en GCP?

Después de iniciar sesión en la "Consola de Google Cloud", los datos de su cuenta de servicio se encuentran en la sección **IAM y Admin**. Para obtener información detallada, consulte "cómo configurar Google Cloud para Astra Control".

Me gustaría agregar diferentes clústeres de GKE de diferentes proyectos de GCP. ¿Es compatible con Astra Control?

No, no es una configuración compatible. Solo se admite un único proyecto de GCP.

Quitar clústeres

¿Cómo cancelo correctamente el registro, elimino un clúster y los volúmenes asociados?

1. "Desgestione las aplicaciones desde Astra Control".
2. "Cancele el registro del clúster de Astra Control".
3. "Elimine las reclamaciones de volumen persistente".
4. Elimine el clúster.

¿Qué ocurre con mis aplicaciones y datos después de quitar el clúster de Astra Control?

La eliminación de un clúster de Astra Control no realizará ningún cambio en la configuración del clúster (aplicaciones y almacenamiento persistente). Las instantáneas de Astra Control o las copias de seguridad tomadas de las aplicaciones en ese clúster no estarán disponibles para restaurar. No se eliminarán los datos de las copias de Snapshot de volumen almacenados en el back-end de almacenamiento. Los backups de almacenamiento persistente creados por Astra Control permanecerán en el almacén de objetos de su proveedor de cloud, pero no podrán restaurarse.

> Quite siempre un clúster de Astra Control antes de eliminarlo mediante GCP. La eliminación de un clúster de GCP mientras Astra Control sigue administrándolo puede causar problemas para su cuenta Astra Control.

¿Astra Control Provisioner se desinstala automáticamente de un clúster cuando lo desgestiono?

Cuando se desgestiona un clúster de Astra Control Center, el aprovisionador de Astra Control o Astra Trident no se desinstalan automáticamente del clúster. Para desinstalar Astra Control Provisioner y sus componentes o Astra Trident, deberá hacerlo "Siga estos pasos para desinstalar la instancia de Astra Trident que contiene el servicio de aprovisionamiento Astra Control".

Gestionar aplicaciones

¿Puede Astra Control implementar una aplicación?

Astra Control no implementa aplicaciones. Las aplicaciones deben implementarse fuera de Astra Control.

No veo que ninguno de los RVP de mi aplicación esté vinculado a GCP CVS. ¿Qué hay de malo?

El operador Astra Trident establece la clase de almacenamiento predeterminada en `netapp-cvs-perf-premium` Después de que se haya añadido correctamente a Astra Control. Cuando las RVP de una aplicación no están vinculadas a Cloud Volumes Service para Google Cloud, hay varios pasos que pueden seguir:

- Ejecución `kubectl get sc` y compruebe la clase de almacenamiento predeterminada.
- Compruebe el archivo yaml o el gráfico Helm que se utilizó para implementar la aplicación y compruebe si se ha definido una clase de almacenamiento diferente.
- La versión 1.24 y posteriores de GKE no admiten imágenes de nodos basadas en Docker. Compruebe que el tipo de imagen de nodo de trabajo de GKE es `COS_CONTAINERD` Y que el montaje NFS se ha realizado correctamente.

¿Qué sucede con las aplicaciones después de dejar de gestionarlas desde Astra Control?

Se eliminarán todos los backups o las snapshots existentes. Las aplicaciones y los datos siguen estando disponibles. Las operaciones de administración de datos no estarán disponibles para aplicaciones no administradas o para cualquier copia de seguridad o copia Snapshot que pertenezcan a él.

Operaciones de gestión de datos

¿Dónde crea Astra Control el bloque de almacén de objetos?

La geografía del primer clúster gestionado determina la ubicación del almacén de objetos. Por ejemplo, si el primer clúster que usted agrega está en una zona europea, entonces el bloque se crea en esa misma geografía. Si es necesario, puede "añadir cucharones adicionales".

Hay instantáneas en mi cuenta que no he creado. ¿De dónde vinieron?

En algunas situaciones, Astra Control creará automáticamente una instantánea como parte de la realización de otro proceso. Si estas instantáneas tienen más de unos minutos de antigüedad, puede eliminarlas de forma segura.

Mi aplicación utiliza varios VP. ¿Deberá Astra Control tomar snapshots y backups de todos estos RVP?

Sí. Una operación de instantánea en una aplicación de Astra Control incluye una instantánea de todos los VP vinculados a las RVP de la aplicación.

¿Puedo gestionar las snapshots tomadas por Astra Control directamente a través de mi proveedor de cloud?

No Las copias Snapshot y los backups que realice Astra Control solo pueden gestionarse con Astra Control.

Aprovisionador de Astra Control

¿En qué se diferencian las funciones de aprovisionamiento de almacenamiento de Astra Control Provisioner de las de Astra Trident?

Astra Control Provisioning, como parte de Astra Control, es compatible con un superconjunto de funciones de aprovisionamiento de almacenamiento que no están disponibles en Astra Trident de código abierto. Estas funciones se suman a todas las funciones que están disponibles en Trident de código abierto.

¿El aprovisionador de Astra Control está reemplazando a Astra Trident?

Astra Control Provisioning ha reemplazado a Astra Trident como aprovisionador de almacenamiento y orquestador en la arquitectura de Astra Control. Los usuarios de Astra Control deberían hacerlo "Habilita el aprovisionador de Astra Control" Para utilizar Astra Control. Astra Trident seguirá siendo compatible en esta versión, pero no será compatible en futuras versiones. Astra Trident seguirá siendo de código abierto y se lanzará, mantendrá, admitirá y actualizará con las nuevas CSI y otras funciones de NetApp. Sin embargo, solo el aprovisionador de Astra Control que contenga la funcionalidad CSI de Astra Trident junto con funcionalidades ampliadas de gestión del almacenamiento pueden usarse con próximas versiones de Astra Control.

¿Tengo que pagar por Astra Trident?

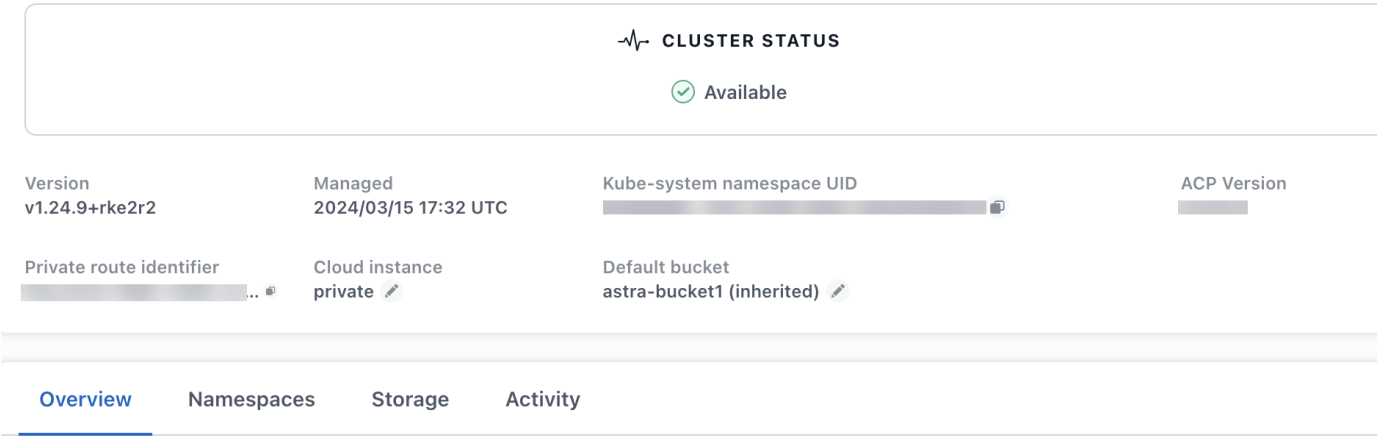
No Astra Trident seguirá siendo de código abierto y puede descargarse gratuitamente. El uso de la funcionalidad de aprovisionamiento de Astra Control ahora requiere una licencia de Astra Control.

¿Puedo usar las funciones de gestión y aprovisionamiento del almacenamiento en Astra Control sin tener que instalar y utilizar todo Astra Control?

Sí, puede actualizar a Astra Control Provisioner y utilizar su funcionalidad aunque no quiera consumir el conjunto de funciones completo de la funcionalidad de gestión de datos de Astra Control.

¿Cómo sé si el aprovisionador de Astra Control ha reemplazado a Astra Trident en mi clúster?

Después de instalar el aprovisionador de Astra Control, el clúster de host de la interfaz de usuario de Astra Control mostrará un `ACP version` en lugar de `Trident version` campo y núm. de versión instalada actual.



Si no tiene acceso a la interfaz de usuario, puede confirmar que la instalación se ha realizado correctamente mediante los siguientes métodos:

Operador Astra Trident

Compruebe el `trident-acp` container se está ejecutando y eso `acpVersion` es `23.10.0` o posterior con el estado de `Installed`:

```
kubectl get torc -o yaml
```

Respuesta:

```
status:
  acpVersion: 23.10.0
  currentInstallationParams:
    ...
    acpImage: <my_custom_registry>/trident-acp:v23.10.0
    enableACP: "true"
    ...
  ...
  status: Installed
```

tridentctl

Confirme que se ha habilitado el aprovisionador de Astra Control:

```
./tridentctl -n trident version
```

Respuesta:

```
+----------------+----------------+-------------+ | SERVER VERSION |
CLIENT VERSION | ACP VERSION | +----------------+----------------
+-------------+ | 23.10.0 | 23.10.0 | 23.10.0. | +----------------
+----------------+-------------+
```

Avisos legales

Los avisos legales proporcionan acceso a las declaraciones de copyright, marcas comerciales, patentes y mucho más.

Derechos de autor

"https://www.netapp.com/company/legal/copyright/"

Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Los demás nombres de empresas y productos son marcas comerciales de sus respectivos propietarios.

"https://www.netapp.com/company/legal/trademarks/"

Estadounidenses

Puede encontrar una lista actual de las patentes propiedad de NetApp en:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidad

"https://www.netapp.com/company/legal/privacy-policy/"

Código abierto

Los archivos de notificación proporcionan información sobre los derechos de autor y las licencias de terceros que se utilizan en software de NetApp.

"Aviso para Astra"

Licencia Astra Control API

https://docs.netapp.com/us-en/astra-automation/media/astra-api-license.pdf