



Conceptos

Astra Control Service

NetApp
June 04, 2024

Tabla de contenidos

- Conceptos 1
 - Arquitectura y componentes 1
 - Protección de datos 6
 - Tipos de almacenamiento y rendimiento para clústeres de AWS 7
 - Clases de almacenamiento y tamaño VP para clústeres AKS. 8
 - Tipo de servicio, clases de almacenamiento y tamaño VP para clústeres GKE 9
 - Gestión de aplicaciones 12
 - Roles de usuario y espacios de nombres 14

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

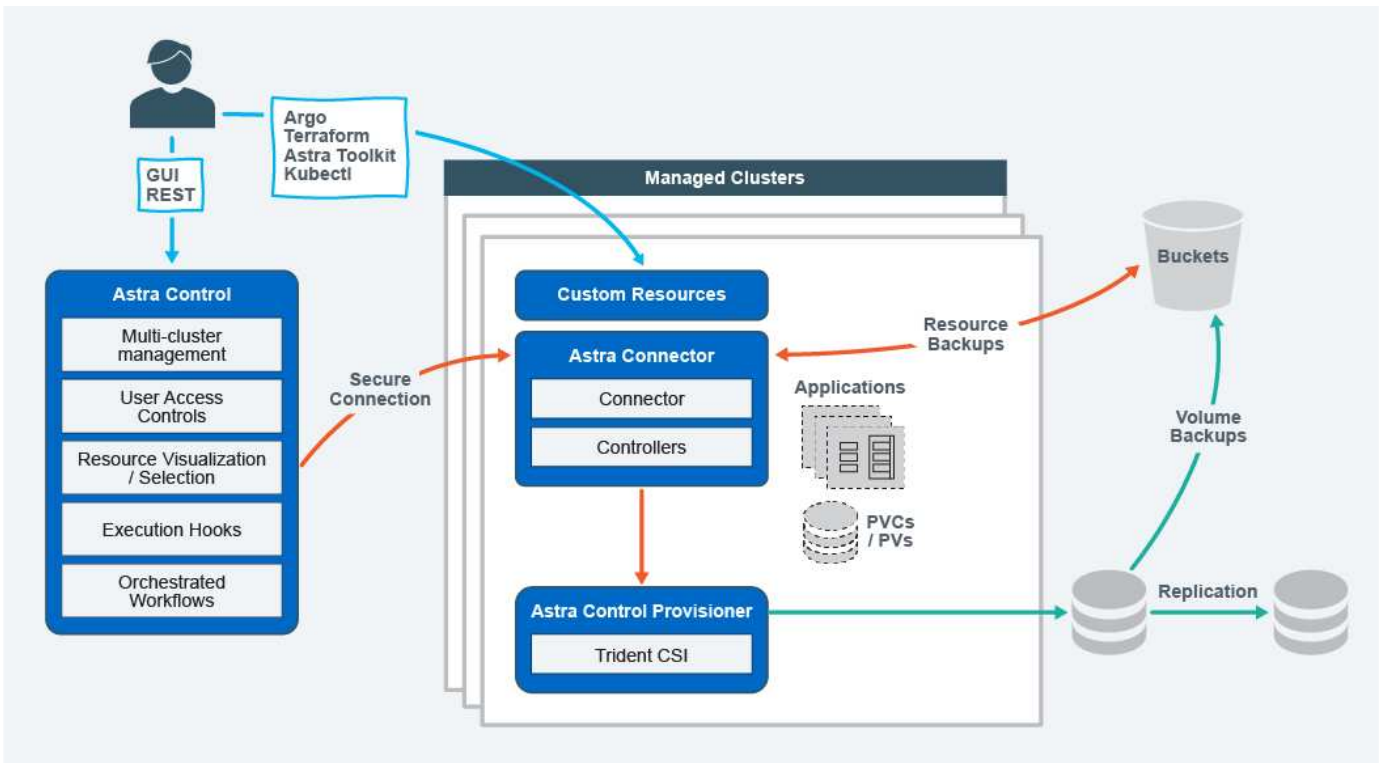
Mover:

- 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:

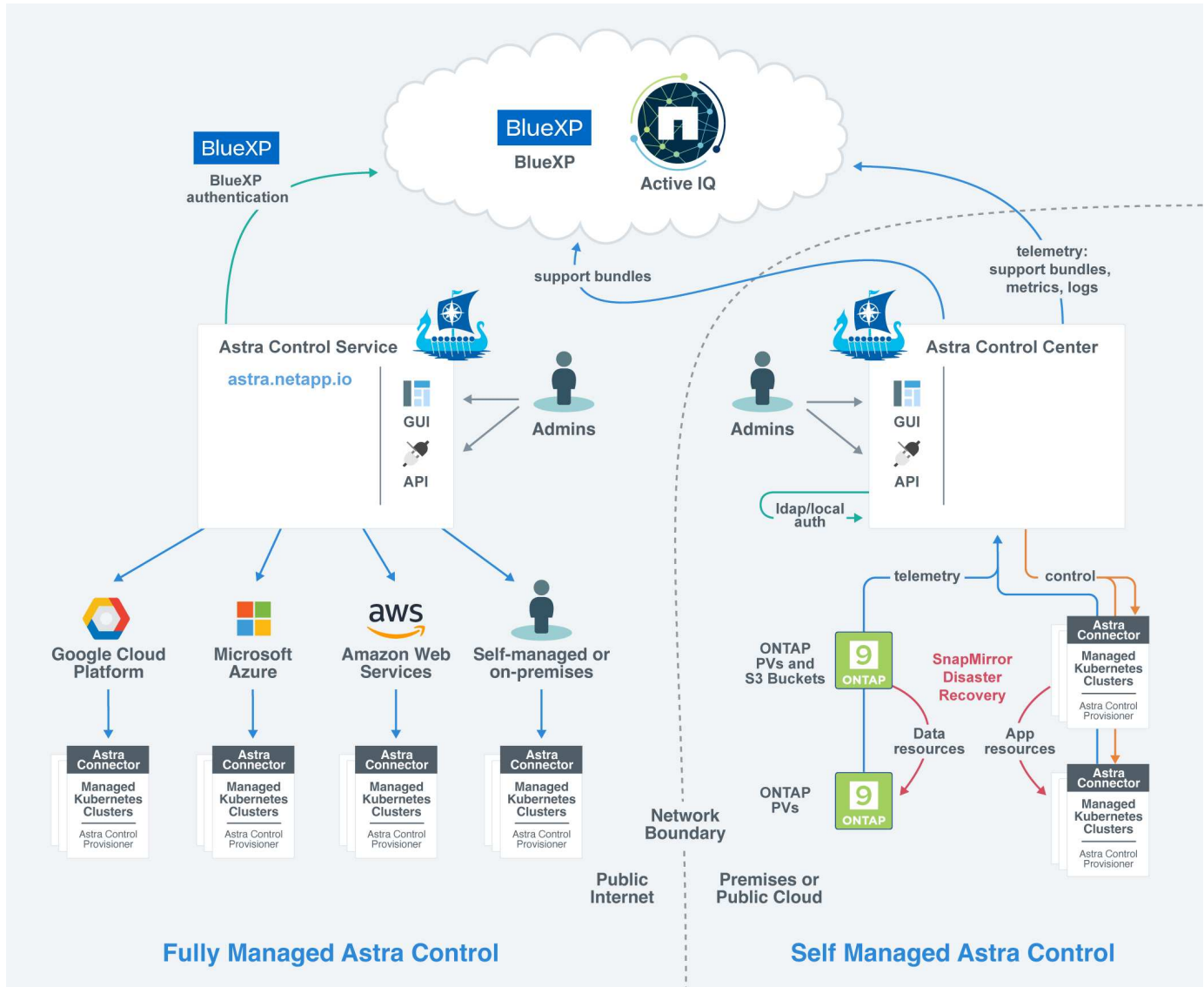
- **Astra Control:** Astra Control es el servicio de gestión centralizado para todos los clústeres gestionados, proporcionando cargas de trabajo orquestadas para la protección y movilidad de aplicaciones en la nube y on-premises, así como las siguientes capacidades:
 - Vista combinada de varios clústeres 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?	<ul style="list-style-type: none"> • * Proveedores en la nube* <ul style="list-style-type: none"> ◦ Amazon Web Services <ul style="list-style-type: none"> ▪ Amazon Elastic Kubernetes Service (EKS) ◦ Google Cloud <ul style="list-style-type: none"> ▪ Google Kubernetes Engine (GKE) ◦ Microsoft Azure <ul style="list-style-type: none"> ▪ Azure Kubernetes Service (AKS) • Clusters autogestionados <ul style="list-style-type: none"> ◦ Kubernetes (ascendente) ◦ Motor Kubernetes de rancher (RKE) ◦ OpenShift Container Platform de Red Hat • * Clústeres locales* <ul style="list-style-type: none"> ◦ Red Hat OpenShift Container Platform en las instalaciones 	<ul style="list-style-type: none"> • 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?	<ul style="list-style-type: none"> • * Proveedores en la nube* <ul style="list-style-type: none"> ◦ Amazon Web Services <ul style="list-style-type: none"> ▪ Amazon EBS ▪ Amazon FSX para ONTAP de NetApp ▪ "Cloud Volumes ONTAP" ◦ Google Cloud <ul style="list-style-type: none"> ▪ Disco persistente de Google ▪ Cloud Volumes Service de NetApp ▪ "Cloud Volumes ONTAP" ◦ Microsoft Azure <ul style="list-style-type: none"> ▪ Discos gestionados de Azure ▪ Azure NetApp Files ▪ "Cloud Volumes ONTAP" • Clusters autogestionados <ul style="list-style-type: none"> ◦ Amazon EBS ◦ Discos gestionados de Azure ◦ Disco persistente de Google ◦ "Cloud Volumes ONTAP" ◦ NetApp MetroCluster ◦ "El Longhorn" • * Clústeres locales* <ul style="list-style-type: none"> ◦ NetApp MetroCluster ◦ Sistemas ONTAP AFF y FAS de NetApp ◦ ONTAP Select de NetApp ◦ "Cloud Volumes ONTAP" ◦ "El Longhorn" 	<ul style="list-style-type: none"> • 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"](#)

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 provisionado 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."	<ul style="list-style-type: none">• 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"](#).

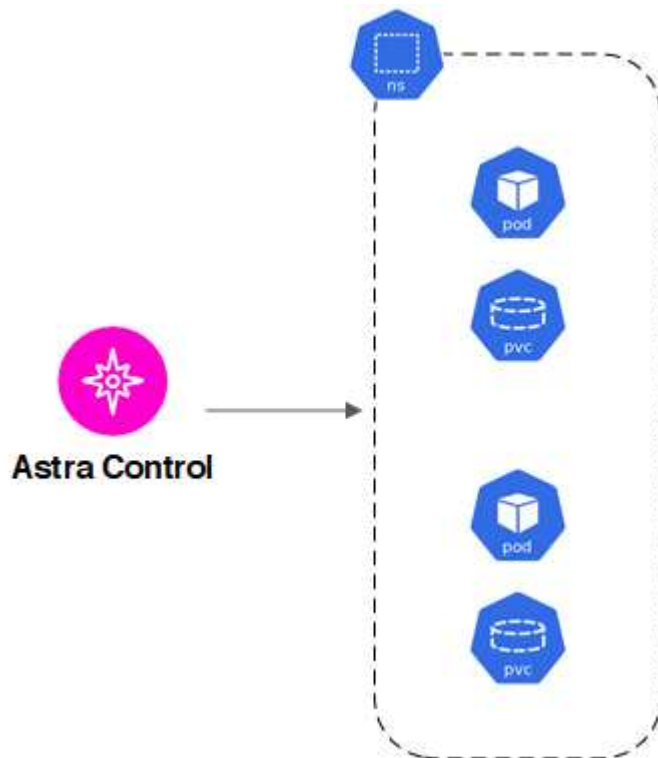
Cloud Volumes ONTAP de NetApp

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"](#).

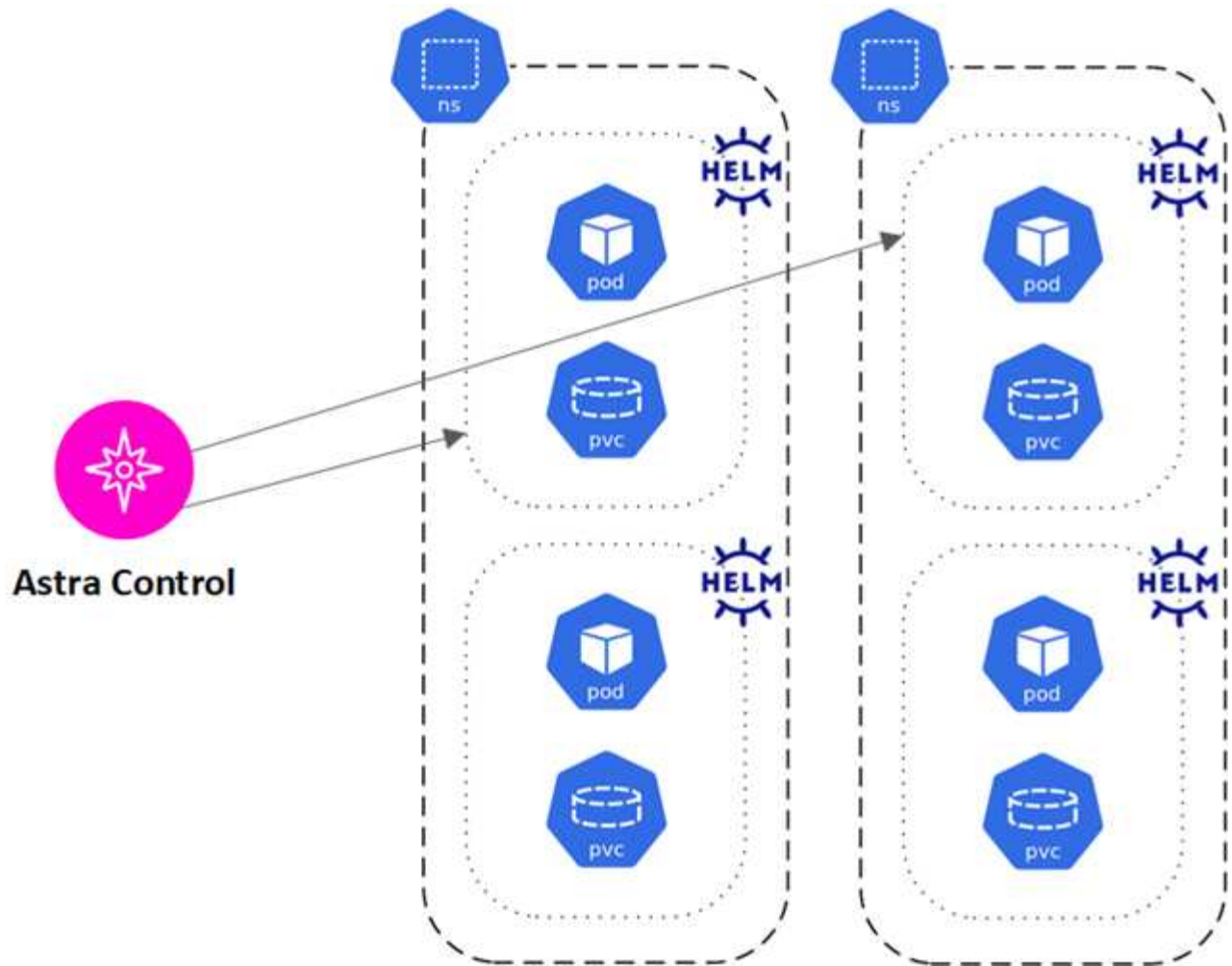
Gestión de aplicaciones

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:

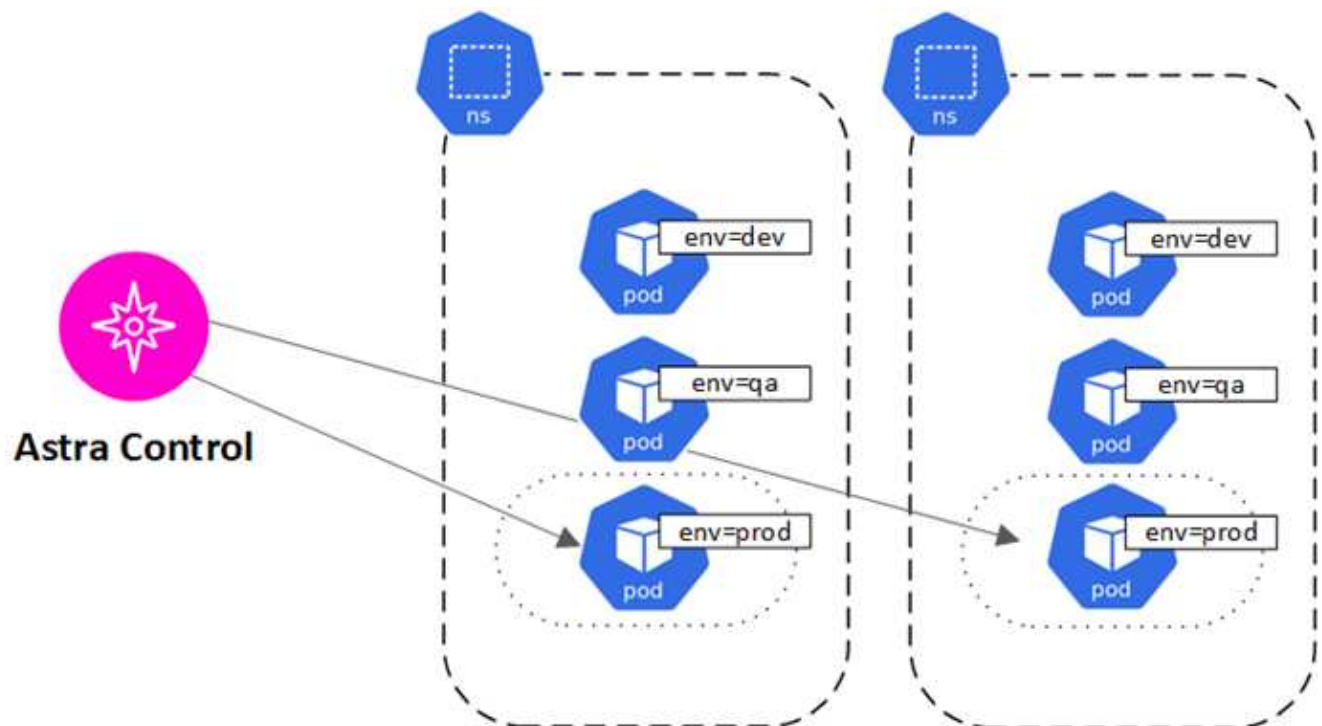
- Un espacio de nombres, incluidos todos los recursos de ese espacio de nombres



- 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"](#)

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.