



Gestionar aplicaciones

Astra Control Center

NetApp

November 21, 2023

Tabla de contenidos

- Gestionar aplicaciones 1
 - Inicie la gestión de aplicaciones 1
 - Defina un ejemplo de aplicación personalizada 7

Gestionar aplicaciones

Inicie la gestión de aplicaciones

Usted primero ["Añada un clúster a la gestión de Astra Control"](#), Puede instalar aplicaciones en el clúster (fuera de Astra Control) y, a continuación, ir a la página aplicaciones de Astra Control para empezar a gestionar las aplicaciones y sus recursos.

Requisitos de gestión de aplicaciones

Astra Control tiene los siguientes requisitos de gestión de aplicaciones:

- **Licencia:** Para gestionar aplicaciones mediante Astra Control Center, necesita una licencia Astra Control Center.
- **Namespaces:** Astra Control requiere que una aplicación no abarque más de un único espacio de nombres, pero un espacio de nombres puede contener más de una aplicación.
- **StorageClass:** Si instala una aplicación con un StorageClass definido explícitamente y necesita clonar la aplicación, el clúster de destino para la operación de clonado debe tener el StorageClass especificado originalmente. Se producirá un error al clonar una aplicación con un tipo de almacenamiento establecido explícitamente en un clúster que no tenga el mismo tipo 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:
 - Función de clúster
 - ClusterRoleBinding
 - ConfigMap
 - CustomResourceDefinition
 - Recurso personalizado
 - DemonSet
 - Puesta en marcha
 - DeploymentConfig
 - Entrada
 - MutatingWebhook
 - Claim persistente
 - Pod
 - Replicaset
 - RoleBinding
 - Función
 - Ruta
 - Secreto
 - Servicio
 - ServiceAccount

- Statilusionados Set
- ValidadoWebhook

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. 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"](#)
 - ["Jenkins CI"](#)
 - ["Clúster Percona XtraDB"](#)

Tenga en cuenta que Astra Control podría 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.



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.

Instale las aplicaciones en el clúster

Ahora que ha agregado su clúster a Astra Control, puede instalar aplicaciones o gestionar las aplicaciones existentes en el clúster. Se puede gestionar cualquier aplicación que esté delimita a un espacio de nombres. Una vez que las POD estén en línea, puede gestionar la aplicación con Astra Control.

Para obtener ayuda sobre la puesta en marcha de aplicaciones validadas de los gráficos Helm, consulte lo siguiente:

- ["Desplegar MariaDB desde un gráfico Helm"](#)
- ["Implemente MySQL desde un gráfico Helm"](#)
- ["Despliegue Postgres desde un gráfico de Helm"](#)
- ["Implemente Jenkins a partir de un gráfico Helm"](#)

Gestionar aplicaciones

Astra Control le permite gestionar sus aplicaciones a nivel de espacio de nombres o mediante etiqueta de Kubernetes.



Las aplicaciones instaladas con Helm 2 no son compatibles.

Puede realizar las siguientes actividades para gestionar aplicaciones:

- Gestionar aplicaciones
 - [Gestionar aplicaciones por espacio de nombres](#)
 - [Gestione aplicaciones mediante la etiqueta Kubernetes](#)
- [Ignorar aplicaciones](#)
- [Desgestionar aplicaciones](#)



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. Para ver las aplicaciones del sistema, utilice el filtro "Mostrar aplicaciones del sistema".

Para obtener instrucciones sobre cómo gestionar aplicaciones mediante la API de Astra Control, consulte ["Información sobre API y automatización de Astra"](#).



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.

Gestionar aplicaciones por espacio de nombres

La sección **descubierto** de la página aplicaciones muestra espacios de nombres y cualquier aplicación instalada en Helm o aplicaciones personalizadas etiquetadas en esos espacios de nombres. Puede optar por gestionar cada aplicación por separado o a nivel de espacio de nombres. Todo se reduce al nivel de granularidad que necesita para las operaciones de protección de datos.

Por ejemplo, puede que desee configurar 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 en un solo espacio de nombres.

Mientras que Astra Control permite gestionar por separado ambos niveles de la jerarquía (el espacio de nombres y las aplicaciones de ese espacio de nombres), la mejor práctica 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.

Pasos

1. En la barra de navegación izquierda, seleccione **aplicaciones**.
2. Seleccione **descubierto**.

Name	Ready	Cluster	Group	Discovered	Actions
default	✓	sc	grp_default	2021/06/28 17:36 UTC	Managed
default1	✓	sc	grp1_default	2021/06/28 17:36 UTC	Unmanaged
default2	✓	sc	grp2_default	2021/06/28 17:36 UTC	Unmanaged
netapp-acc-operator	✓	sc	netapp-acc-operator	2021/07/13 12:36 UTC	Unmanaged
pcloud	✓	sc	pcloud	2021/07/13 12:37 UTC	Unmanaged

- Consulte la lista de espacios de nombres detectados. Amplíe el espacio de nombres para ver las aplicaciones y los recursos asociados.

Astra Control le muestra las aplicaciones Helm y las aplicaciones personalizadas en el espacio de nombres. Si hay etiquetas Helm disponibles, se designarán con un icono de etiqueta.

- Observe la columna **Grupo** para ver en qué espacio de nombres se está ejecutando la aplicación (está designada con el icono de carpeta).
- Decida si desea gestionar cada aplicación de forma individual o a nivel de espacio de nombres.
- Busque la aplicación que desee en el nivel deseado en la jerarquía y, en el menú acciones, seleccione **gestionar**.
- Si no desea gestionar una aplicación, en el menú acciones situado junto a la aplicación, seleccione **ignorar**.

Por ejemplo, si desea gestionar juntas todas las aplicaciones del espacio de nombres "maría" para que tengan las mismas políticas de copia Snapshot y copia de seguridad, debe gestionar el espacio de nombres e ignorar las aplicaciones del espacio de nombres.

- Para ver la lista de aplicaciones administradas, seleccione **gestionado** como filtro de visualización.

Name	Ready	Protected	Cluster	Group	Discovered	Actions
appf	✓	ⓘ	sc	app-logging	2021/06/28 17:36 UTC	Available

Observe que la aplicación que acaba de agregar tiene un icono de advertencia debajo de la columna protegida, 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.

Resultado

Las aplicaciones que eligió administrar ahora están disponibles en la pestaña **gestionado**. Cualquier aplicación ignorada se moverá a la pestaña **ignorada**. Lo ideal es que la ficha descubierto no muestre

ninguna aplicación, de modo que, a medida que se instalan nuevas aplicaciones, resulta más fácil encontrarlos y gestionarlos.

Gestione aplicaciones mediante la etiqueta Kubernetes

Astra Control incluye una acción en la parte superior de la página de aplicaciones llamada **definir aplicación personalizada**. Puede usar esta acción para gestionar las aplicaciones identificadas con una etiqueta de Kubernetes. "[Obtenga más información sobre cómo definir aplicaciones personalizadas mediante etiqueta de Kubernetes](#)".

Pasos

1. En la barra de navegación izquierda, seleccione **aplicaciones**.
2. Seleccione **definir**.

3. En el cuadro de diálogo **definir aplicación personalizada**, proporcione la información necesaria para administrar la aplicación:
 - a. **Nueva aplicación:** Introduzca el nombre para mostrar de la aplicación.
 - b. **Cluster:** Seleccione el clúster en el que reside la aplicación.
 - c. **espacio de nombres:** Seleccione el espacio de nombres para la aplicación.
 - d. **etiqueta:** Introduzca una etiqueta o seleccione una de las siguientes fuentes.
 - e. **Recursos seleccionados:** Vea y gestione los recursos de Kubernetes seleccionados que le gustaría proteger (pods, secretos, volúmenes persistentes, etc.).
 - Para ver las etiquetas disponibles, amplíe un recurso y seleccione el número de etiquetas.
 - Seleccione una de las etiquetas.

Después de seleccionar una etiqueta, se muestra en el campo **etiqueta**. Astra Control también actualiza la sección **Recursos no seleccionados** para mostrar los recursos que no coinciden con la etiqueta seleccionada.

f. **Recursos no seleccionados**: Verifique los recursos de la aplicación que no desea proteger.

4. Seleccione **definir aplicación personalizada**.

Resultado

Astra Control permite la gestión de la aplicación. Ahora puede encontrarlo en la pestaña **gestionado**.

Ignorar aplicaciones

Si se ha detectado una aplicación, ésta aparece en la lista descubierta. En este caso, puede limpiar la lista descubierta para que las nuevas aplicaciones que se han instalado sean más fáciles de encontrar. O bien, puede que tenga aplicaciones que esté gestionando y, más adelante, decida que ya no desea gestionarla. Si no desea administrar estas aplicaciones, puede indicar que deben ignorarse.

Además, puede que desee gestionar aplicaciones en un espacio de nombres (gestionado por espacios de nombres). Puede ignorar las aplicaciones que desea excluir del espacio de nombres.

Pasos

1. En la barra de navegación izquierda, seleccione **aplicaciones**.
2. Seleccione **descubierto** como filtro.
3. Seleccione la aplicación.
4. En el menú acciones, seleccione **Ignorar**.
5. Para designorar, en el menú acciones, seleccione **no ignorar**.

Desgestionar aplicaciones

Cuando ya no desee realizar una copia de seguridad, una instantánea o clonar una aplicación, puede dejar de administrarla.



Si desgestiona una aplicación, se perderán todos los backups o las instantáneas que se hayan creado anteriormente.

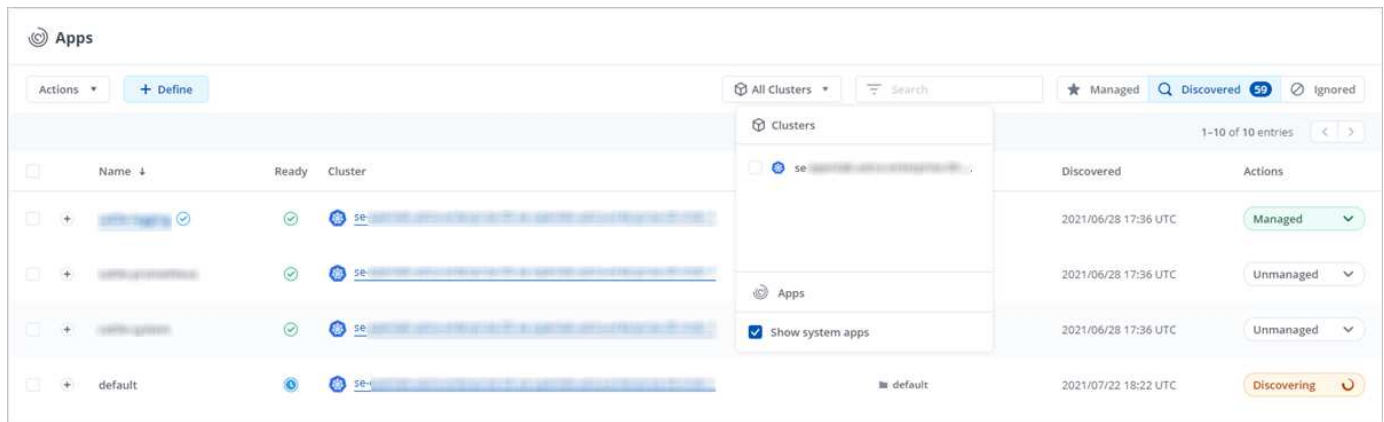
Pasos

1. En la barra de navegación izquierda, seleccione **aplicaciones**.
2. Seleccione **gestionado** como filtro.
3. Seleccione la aplicación.
4. En el menú acciones, seleccione **Unmanage**.
5. Revise la información.
6. Escriba "desgestionar" para confirmar.
7. Seleccione **Sí, Desactivar aplicación**.

¿y las aplicaciones del sistema?

Astra Control también detecta las aplicaciones del sistema que se ejecutan en un clúster de Kubernetes. Puede mostrar las aplicaciones del sistema seleccionando la casilla de verificación **Mostrar aplicaciones del**

sistema en el filtro de clúster de la barra de herramientas.



No le mostramos estas aplicaciones del sistema de forma predeterminada porque es raro que tenga que hacer una copia de seguridad.



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. Para ver las aplicaciones del sistema, utilice el filtro "Mostrar aplicaciones del sistema".

Obtenga más información

- ["Utilice la API Astra Control"](#)

Defina un ejemplo de aplicación personalizada

Crear una aplicación personalizada le permite agrupar elementos de su clúster de Kubernetes en una única aplicación.

Una aplicación personalizada le ofrece un control más granular de lo que debe incluirse en una operación de Astra Control, entre las que se incluyen:

- Clonar
- Snapshot
- Backup
- Política de protección

En la mayoría de los casos, querrá utilizar las funciones de Astra Control en toda su aplicación. Sin embargo, también puede crear una aplicación personalizada para utilizar estas funciones con las etiquetas que asigne a los objetos de Kubernetes en un espacio de nombres.

Para crear una aplicación personalizada, vaya a la página aplicaciones y seleccione **+ define**.

A medida que realice las selecciones, la ventana aplicación personalizada mostrará los recursos que se incluirán o excluirán de la aplicación personalizada. Esto le ayuda a asegurarse de que está eligiendo los criterios correctos para definir su aplicación personalizada.



Las aplicaciones personalizadas solo se pueden crear dentro de un espacio de nombres especificado en un único clúster. Astra Control no admite la capacidad de una aplicación personalizada para abarcar varios espacios de nombres o clústeres.

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](#)".



Las directivas que se solapan para el mismo recurso con nombres diferentes pueden provocar conflictos de datos. Si crea una aplicación personalizada para un recurso, asegúrese de que no se clona ni se realiza un backup en ninguna otra política.

Ejemplo: Política de protección independiente para el lanzamiento canario

En este ejemplo, el equipo de devops gestiona una puesta en marcha de versiones canaria. Su grupo tiene tres pods que ejecutan nginx. Dos de los pods están dedicados a la versión estable. El tercer pod es para el lanzamiento canario.

El administrador de Kubernetes del equipo de devops añade la etiqueta `deployment=stable` a los pods de liberación estables. El equipo agrega la etiqueta `deployment=canary` a la cápsula de liberación canaria.

La versión estable del equipo incluye los requisitos de snapshots cada hora y backups diarios. la liberación canaria es más efímera, por lo que quieren crear una Política de Protección a corto plazo menos agresiva para cualquier cosa etiquetada `deployment=canary`.

Para evitar posibles conflictos de datos, el administrador creará dos aplicaciones personalizadas: Una para el lanzamiento canario y otra para el lanzamiento estable. De este modo, los backups, las snapshots y las operaciones de clonado se mantienen independientes para los dos grupos de objetos de Kubernetes.

Pasos

1. Una vez que el equipo agrega el clúster a Astra Control, el siguiente paso es definir una aplicación personalizada. Para ello, el equipo selecciona el botón **+ define** de la página aplicaciones.
2. En la ventana emergente que aparece, el equipo establece `devops-canary-deployment` como nombre de la aplicación. El equipo elige el cluster en la lista desplegable **Cluster**, entonces el espacio de nombres de la aplicación del menú desplegable **namespace**.
3. El equipo puede escribir `deployment=canary` En el campo **Etiquetas**, o seleccione esa etiqueta de los recursos que se muestran a continuación.
4. Después de definir la aplicación personalizada para la implementación canaria, el equipo repite el proceso para la implementación estable.

Cuando el equipo haya terminado de crear las dos aplicaciones personalizadas, pueden tratar estos recursos como cualquier otra aplicación de Astra Control. Pueden clonarlas, crear backups y snapshots, y crear una política de protección personalizada para cada grupo de recursos basada en las etiquetas de Kubernetes.

Información de copyright

Copyright © 2023 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.