



DevOps con NetApp Astra

NetApp Solutions

NetApp
April 25, 2024

This PDF was generated from https://docs.netapp.com/es-es/netapp-solutions/containers/dwn_overview_devops.html on April 25, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

- TR-4919: DevOps con NetApp Astra 1
 - Casos de uso 1
 - Valor empresarial 1
 - Información general de la tecnología 1
 - Información general de DevOps 2
 - Información general de los sistemas de almacenamiento de NetApp 5
 - Descripción general de integración del almacenamiento de NetApp 8
 - Validación de casos prácticos: DevOps con NetApp Astra 11
 - Vídeos y demostraciones: DevOps con NetApp Astra 29
 - Información adicional: DevOps con NetApp Astra 29

TR-4919: DevOps con NetApp Astra

Alan Cowles y Nikhil M Kulkarni, NetApp

Casos de uso

La solución DevOps con NetApp Astra ha sido diseñada para ofrecer un valor excepcional a los clientes con los siguientes casos prácticos:

- Es fácil de poner en marcha y gestionar entornos de aplicaciones y desarrollo implementados sobre las distribuciones de Kubernetes compatibles.
- Discusión de casos prácticos reales para flujos de trabajo de DevOps y ejemplos de herramientas y métodos que puede proporcionar NetApp para facilitar la adopción y el uso de estos métodos.
- Exploración de cómo se pueden usar las copias Snapshot, los backups y los clones coherentes con las aplicaciones para mejorar la experiencia de DevOps.

Valor empresarial

Las empresas están adoptando cada vez más prácticas de DevOps para crear nuevos productos, acortar los ciclos de lanzamiento y agregar nuevas funciones con rapidez. Debido a su naturaleza ágil innata, los contenedores y microservicios tienen un papel crucial en el soporte de las prácticas de DevOps. Sin embargo, practicar DevOps a escala de producción en un entorno empresarial presenta sus propios retos e impone ciertos requisitos sobre la infraestructura subyacente, como los siguientes:

- Alta disponibilidad en todas las capas de la pila, de forma que los flujos de trabajo nunca se interrumpen.
- Facilidad de los procedimientos de puesta en marcha y gestión para el usuario final.
- Infraestructura programable y condicionada por API para seguir el ritmo de los microservicios y la agilidad de los desarrolladores.
- Capacidad de escalar la infraestructura de forma independiente y automatizada en función de las demandas de las cargas de trabajo.
- La protección de aplicaciones junto con sus conjuntos de datos persistentes de backup para flujos de trabajo de DevOps acelera el plazo de comercialización al no tener que depender de la repuesta en marcha o de la copia manual de datos.

Reconociendo estas funcionalidades y retos, este informe técnico describe el proceso de mejorar y simplificar los casos prácticos de DevOps para aplicaciones en contenedores utilizando la amplia cartera de productos de NetApp.

Información general de la tecnología

DevOps con la solución NetApp consta de los siguientes componentes principales:

Prácticas de DevOps

Las prácticas de DevOps se centran en operaciones automatizadas, repetibles y fácilmente gestionables que mejoran el flujo de trabajo del desarrollo, al permitir al usuario final controlar el entorno en el que desarrolla su código. Esta solución proporciona varios ejemplos y casos de uso en los que la tecnología de NetApp puede ser de mayor beneficio para dichas operaciones.

Orquestación de contenedores

Actualmente, existen numerosas plataformas de orquestación de contenedores en uso. Aunque la mayoría de estas plataformas se basan en Kubernetes, cada una tiene un pros y contras. Por lo tanto, es importante comprender los conjuntos de funciones y las integraciones al seleccionar una plataforma de orquestación de contenedores para los flujos de trabajo de DevOps. Con la suite Astra de productos de NetApp, somos compatibles con las siguientes plataformas para los casos prácticos de DevOps completo:

- ["Red Hat OpenShift" 4.6.8+](#)
- ["Guardabosques" 2.5 o posterior](#)
- ["Kubernetes" 1.20 o posterior](#)
- ["Grid de Kubernetes de VMware Tanzania" 1.4 o posterior](#)
- ["VMware Tanzu Kubernetes Grid Integrated Edition" 1.12.2 o posterior](#)

Sistemas de almacenamiento NetApp

NetApp cuenta con varios sistemas de almacenamiento perfectos para centros de datos empresariales y para puestas en marcha de cloud híbrido. La cartera de NetApp incluye sistemas de almacenamiento ONTAP, NetApp Element y E-Series de NetApp, todos los cuales pueden proporcionar almacenamiento persistente para aplicaciones en contenedores.

Si quiere más información, visite el sitio web de NetApp ["aquí"](#).

Integraciones de almacenamiento de NetApp

Astra Control Center de NetApp ofrece un amplio conjunto de servicios de gestión de datos para aplicaciones y almacenamiento para cargas de trabajo con estado de Kubernetes puestas en marcha en un entorno local y con la tecnología de protección de datos de confianza de NetApp.

Si quiere más información, visite el sitio web de Astra de NetApp ["aquí"](#).

Astra Trident es un orquestador de almacenamiento de código abierto y totalmente compatible para contenedores y distribuciones de Kubernetes como Red Hat OpenShift, VMware Tanzu, Anthos by Google Cloud etc..

Si quiere más información, visite el sitio web de Astra Trident ["aquí"](#).

Información general de DevOps

A lo largo de los últimos años, las organizaciones que crean software han ido adoptando los conceptos de DevOps. Las prácticas de DevOps eliminan las barreras de la organización y acercan a los equipos de desarrollo y operaciones. Las prácticas de DevOps también permiten a los equipos acelerar la entrega, aumentar la disponibilidad y lograr que los servicios y las aplicaciones sean más estables; de este modo, se mejora la productividad del equipo. Además, la adopción de un marco de automatización también es una característica clave del éxito: Desde la creación, la prueba y el funcionamiento de aplicaciones a escala o la gestión de una plataforma o una pila de infraestructura completamente automatizada. A continuación comentamos algunos casos prácticos principales de DevOps en los que se pueden implementar las soluciones de NetApp para

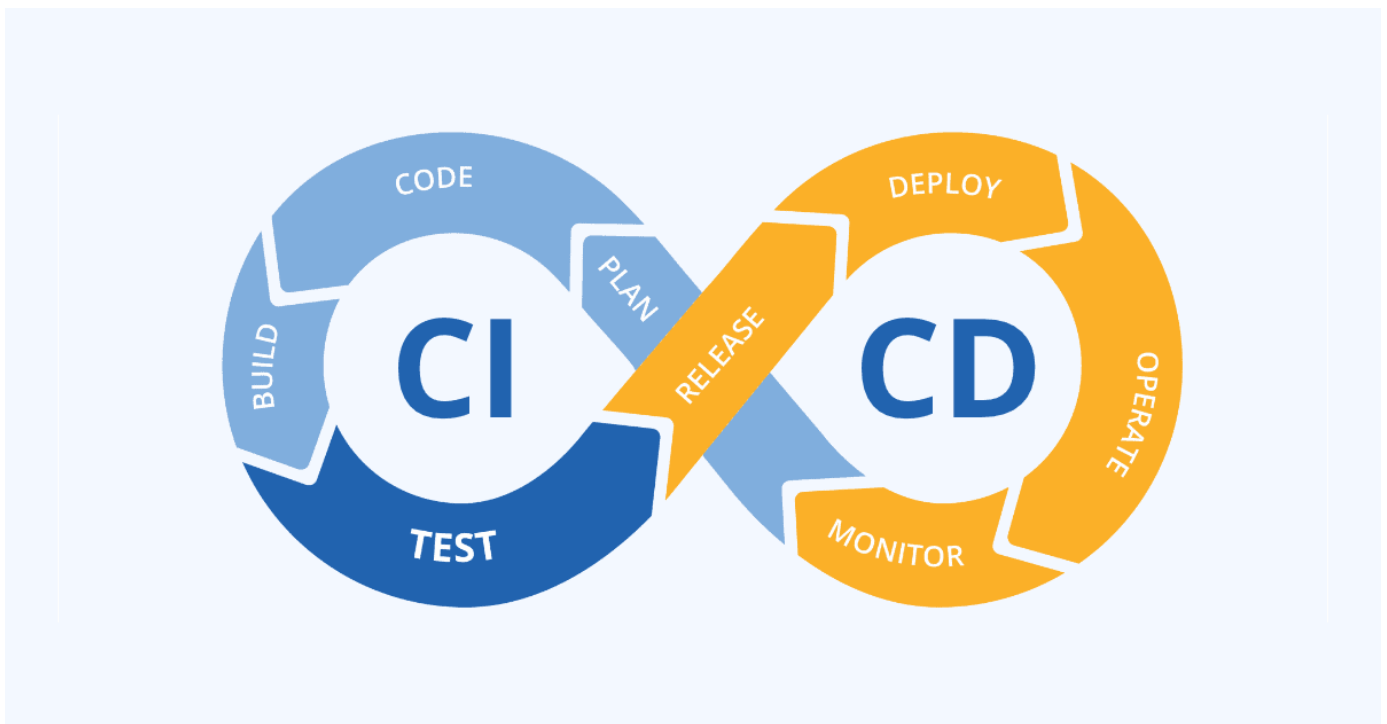
ayudar a mejorar las experiencias que los profesionales de DevOps encuentran durante su práctica diaria.

Casos de uso de DevOps

Aunque DevOps no tiene una definición única y universalmente aceptada, las soluciones para los practicantes de DevOps suelen contener construcciones o ideologías similares que permiten una implementación, repetición y gestión sencillas a escala. En las siguientes secciones se describen posibles casos de uso para los flujos de trabajo de DevOps que ofrecen las soluciones de NetApp.

Integración continua, entrega continua e implementación continua (CI/CD)

Integración continua, entrega continua e implementación continua (CI/CD) es una filosofía de codificación que anima a los desarrolladores a implementar y transformar sus prácticas de codificación mediante el establecimiento de un método mediante el cual pueden actualizar, probar e implementar su código de manera automatizada y coherente. El método más popular por el que se implementa CI/CD en la mayoría de los flujos de trabajo de DevOps es el de la canalización de CI/CD y existen varias aplicaciones de software de terceros que pueden ayudar a conseguirlo.



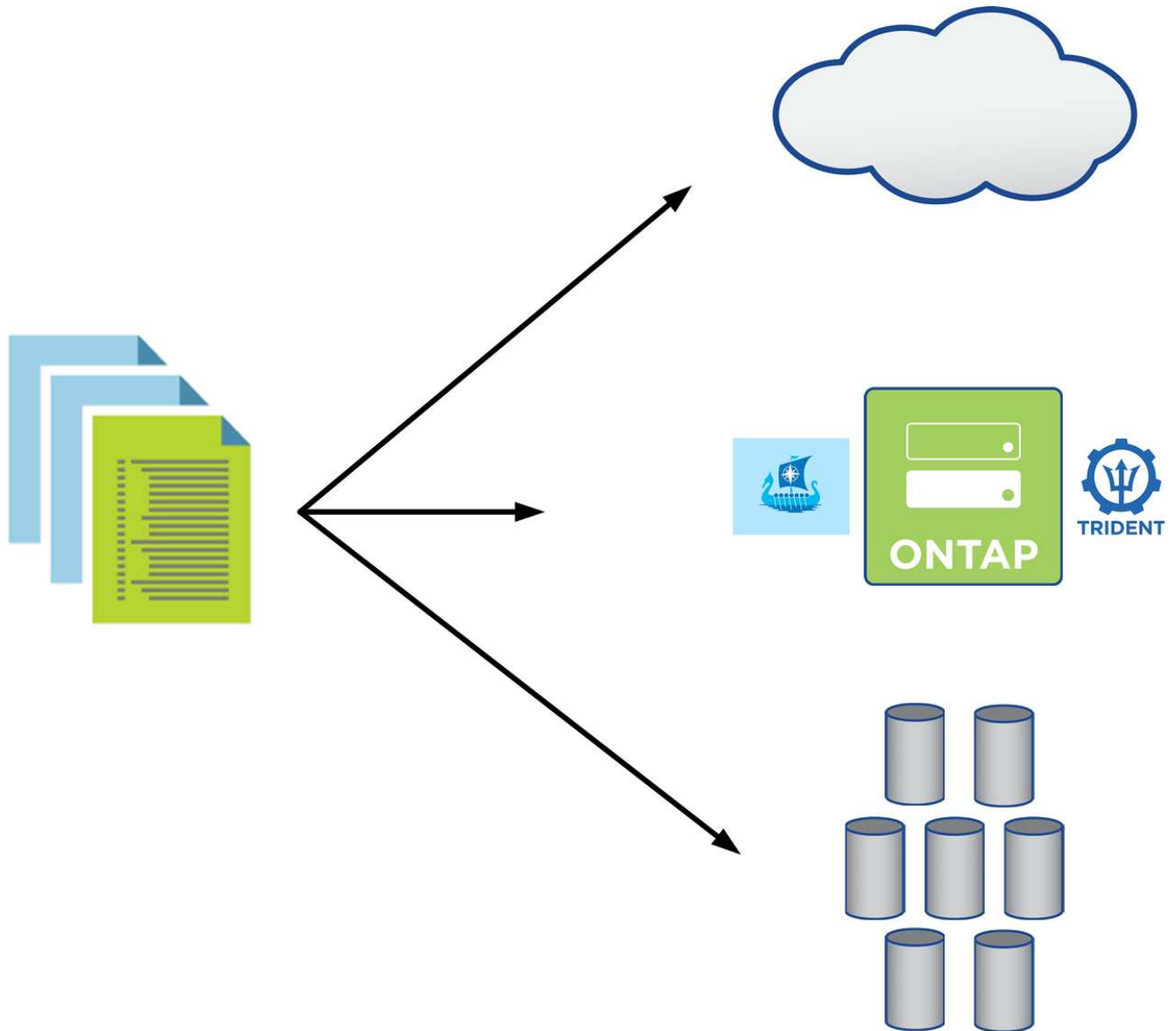
Consulte los siguientes ejemplos de aplicaciones conocidas que pueden ayudar con los flujos de trabajo de tipo CI/CD:

"ArgoCD"
"Jenkins"
"Tekton"

Algunos de los casos de uso incluidos más adelante en este informe técnico se han demostrado en Jenkins, pero los principios fundamentales de CI/CD pueden aplicarse a cualquier herramienta que una organización haya implementado en sus propias prácticas.

Infraestructura como código

La infraestructura como código ayuda a aprovisionar y gestionar recursos TECNOLÓGICOS mediante comandos automatizados, API y kits de desarrollo de software (SDK). Este concepto mejora considerablemente la experiencia de DevOps al eliminar las limitaciones de recursos o centros de datos físicos que podrían impedir que los desarrolladores cumplieran sus objetivos.

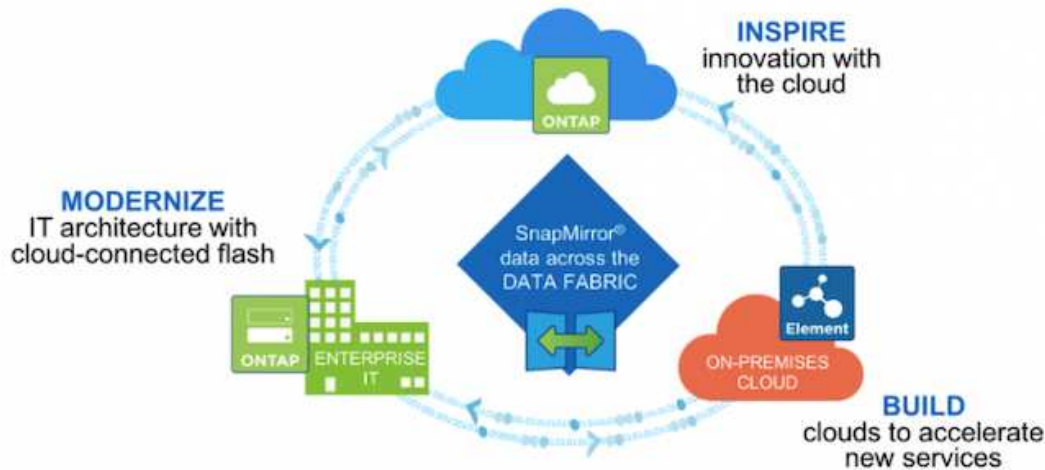


Los usuarios finales suelen utilizar lenguajes de programación como **"Python"** o herramientas de automatización como **"Ansible"** o **"Puppet"** para crear acciones de escalado de infraestructura automatizadas y repetibles que pueden llamar los desarrolladores cuando sea necesario.

Tanto ONTAP de NetApp como Astra Control contienen API que se enfrentan al público y módulos de Ansible o kits de herramientas de desarrollo de software que facilitan la automatización de las operaciones y la integración en los procesos de DevOps.

Información general de los sistemas de almacenamiento de NetApp

NetApp cuenta con varias plataformas de almacenamiento cualificadas con Astra Trident y Astra Control para aprovisionar, proteger y gestionar datos para aplicaciones en contenedores.



- Los sistemas AFF y FAS ejecutan ONTAP de NetApp y proporcionan almacenamiento para casos de uso basados en archivos (NFS) y basados en bloques (iSCSI).
- Cloud Volumes ONTAP y ONTAP Select proporcionan las mismas ventajas en el espacio cloud y virtual respectivamente.
- NetApp Cloud Volumes Service (AWS/GCP) y Azure NetApp Files proporcionan almacenamiento basado en archivos en el cloud.



Cada sistema de almacenamiento de la cartera de NetApp puede facilitar la gestión y el movimiento de datos entre sitios locales y el cloud para que los datos estén donde están sus aplicaciones.

En las siguientes páginas se ofrece información adicional acerca de los sistemas de almacenamiento de NetApp validados en la solución DevOps with NetApp:

- ["ONTAP de NetApp"](#)

ONTAP de NetApp

ONTAP de NetApp es una potente herramienta de software de almacenamiento con funcionalidades como una interfaz gráfica de usuario intuitiva, API DE REST con integración de automatización, análisis predictivos con información de IA y acciones correctivas, actualizaciones de hardware no disruptivas e importación entre almacenamiento.

Para obtener más información sobre el sistema de almacenamiento ONTAP de NetApp, visite la ["Sitio web de ONTAP de NetApp"](#).

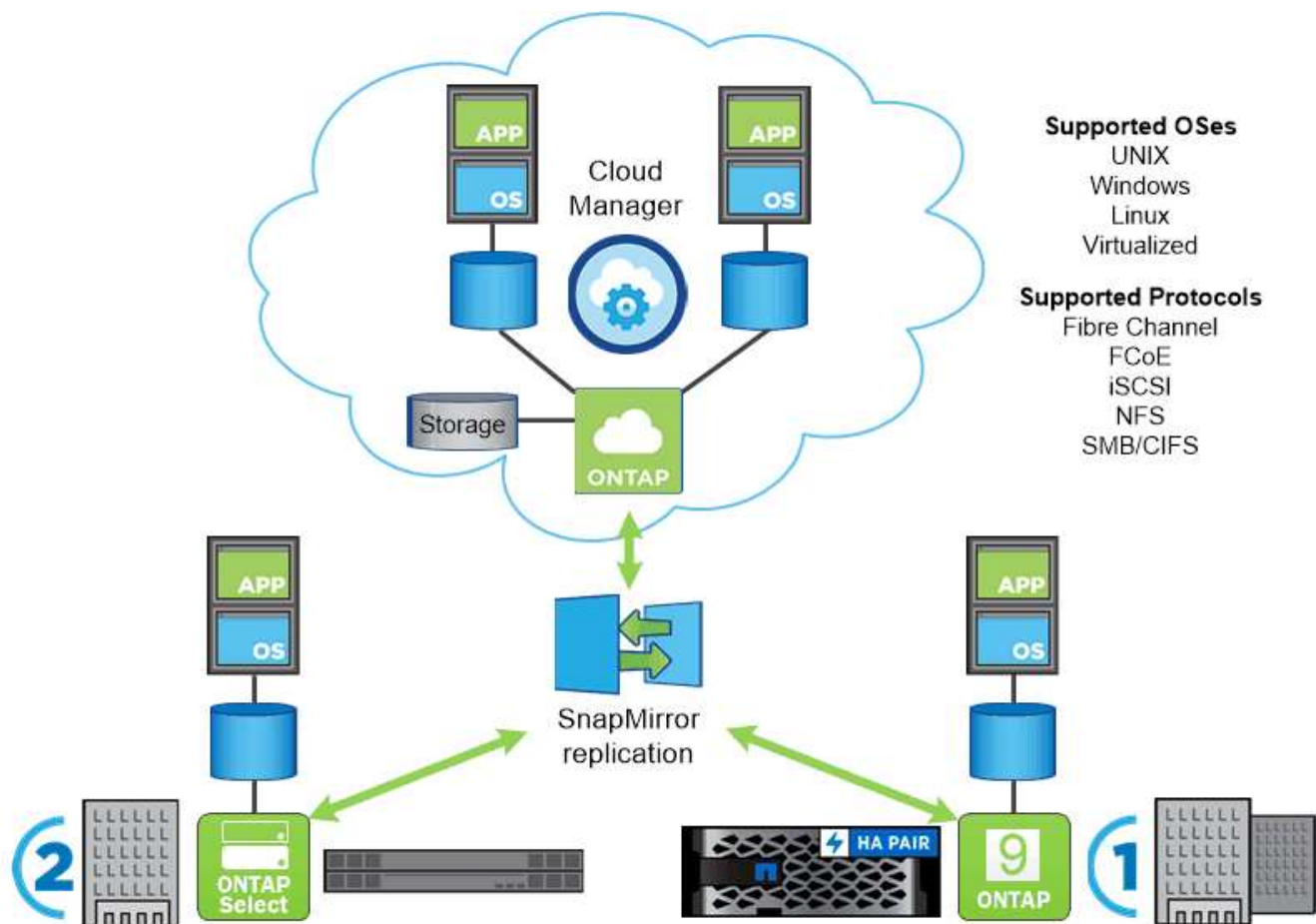
ONTAP ofrece las siguientes funciones:

- Un sistema de almacenamiento unificado con acceso simultáneo a datos y gestión de NFS, CIFS, iSCSI, FC, FCoE, Y los protocolos FC-NVMe.
- Los diferentes modelos de puesta en marcha incluyen configuraciones locales de hardware all-flash, híbrido y all-HDD; plataformas de almacenamiento basadas en máquinas virtuales en un hipervisor compatible, como ONTAP Select; y en el cloud como Cloud Volumes ONTAP.
- Eficiencia del almacenamiento de datos aumentada en los sistemas de ONTAP con compatibilidad para niveles de datos automáticos, compresión de datos inline, deduplicación y compactación.
- Almacenamiento basado en cargas de trabajo controlado por la calidad de servicio.
- Integración fluida con un cloud público para la organización en niveles y la protección de datos. ONTAP también proporciona funcionalidades de protección de datos sólidas que lo diferencian en cualquier entorno:
 - **Copias Snapshot de NetApp.** una copia de seguridad rápida y puntual de los datos con una cantidad mínima de espacio en disco sin sobrecarga adicional del rendimiento.
 - **SnapMirror de NetApp.** duplica las copias Snapshot de los datos de un sistema de almacenamiento a otro. ONTAP también admite el mirroring de datos en otras plataformas físicas y servicios nativos del cloud.
 - **SnapLock de NetApp.** Administración eficaz de datos no regrabables escribiéndolos en volúmenes especiales que no se puedan sobrescribir ni borrar durante un periodo determinado.
 - **SnapVault de NetApp.** realiza un backup de datos de varios sistemas de almacenamiento en una copia snapshot central que sirve de respaldo a todos los sistemas designados.
 - **SyncMirror de NetApp.** proporciona mirroring de datos a nivel de RAID en tiempo real a dos complejos de discos diferentes que están conectados físicamente a la misma controladora.
 - **SnapRestore de NetApp.** proporciona una rápida restauración de los datos de backup bajo demanda a partir de copias snapshot.
 - **FlexClone de NetApp** proporciona el aprovisionamiento instantáneo de una copia totalmente legible y modificable de un volumen NetApp en función de una copia snapshot.

Para obtener más información acerca de ONTAP, consulte ["Centro de documentación de ONTAP 9"](#).



ONTAP de NetApp está disponible en las instalaciones, virtualizado o en el cloud.



Plataformas NetApp

AFF/FAS de NetApp

NetApp proporciona plataformas de almacenamiento sólidas all-flash (AFF) y híbridas de escalado horizontal (FAS) diseñadas a medida con un rendimiento de baja latencia, protección de datos integrada y compatibilidad con varios protocolos.

Ambos sistemas cuentan con el software para la gestión de datos ONTAP de NetApp, el software de gestión de datos más avanzado del sector para una gestión del almacenamiento integrada en el cloud, de alta disponibilidad y simplificada, para ofrecer seguridad, eficiencia y velocidad aptas para el ámbito empresarial que se ajuste a sus necesidades de Data Fabric.

Para obtener más información sobre las plataformas AFF/FAS de NETAPP, haga clic en ["aquí"](#).

ONTAP Select

ONTAP Select es una puesta en marcha definida por software de ONTAP de NetApp que se puede poner en marcha en un hipervisor en su entorno. Puede instalarse en VMware vSphere o en KVM y proporciona todas las funciones y la experiencia de un sistema ONTAP basado en hardware.

Para obtener más información acerca de ONTAP Select, haga clic en ["aquí"](#).

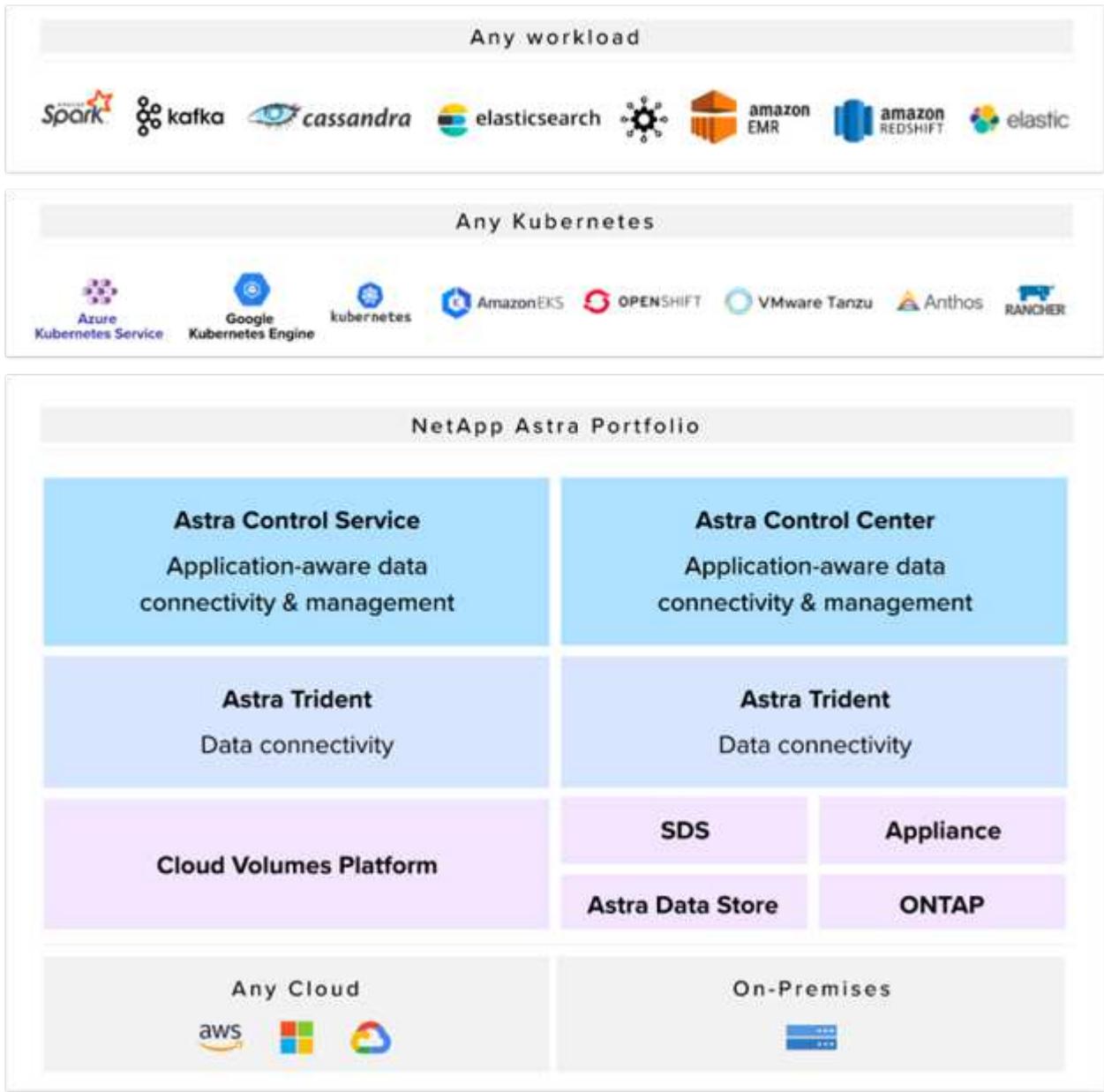
Cloud Volumes ONTAP

Cloud Volumes ONTAP de NetApp es una versión de NetApp ONTAP que se puede poner en marcha en un gran número de clouds públicos, incluidos Amazon AWS, Microsoft Azure y Google Cloud.

Para obtener más información acerca de Cloud Volumes ONTAP, haga clic en ["aquí"](#).

Descripción general de integración del almacenamiento de NetApp

NetApp proporciona una serie de productos para ayudarle a orquestar, gestionar, proteger y migrar aplicaciones con contenedores con estado y sus datos.



Astra Control de NetApp ofrece un amplio conjunto de servicios de gestión de datos para aplicaciones y almacenamiento para cargas de trabajo con estado de Kubernetes gracias a la tecnología de protección de datos de NetApp. El servicio Astra Control está disponible para admitir cargas de trabajo con estado en puestas en marcha de Kubernetes nativas para el cloud. Astra Control Center está disponible para admitir

cargas de trabajo con estado en puestas en marcha en las instalaciones de plataformas Enterprise Kubernetes como Red Hat OpenShift, Rancher, VMware Tanzu etc. Si quiere más información, visite el sitio web de Astra Control de NetApp ["aquí"](#).

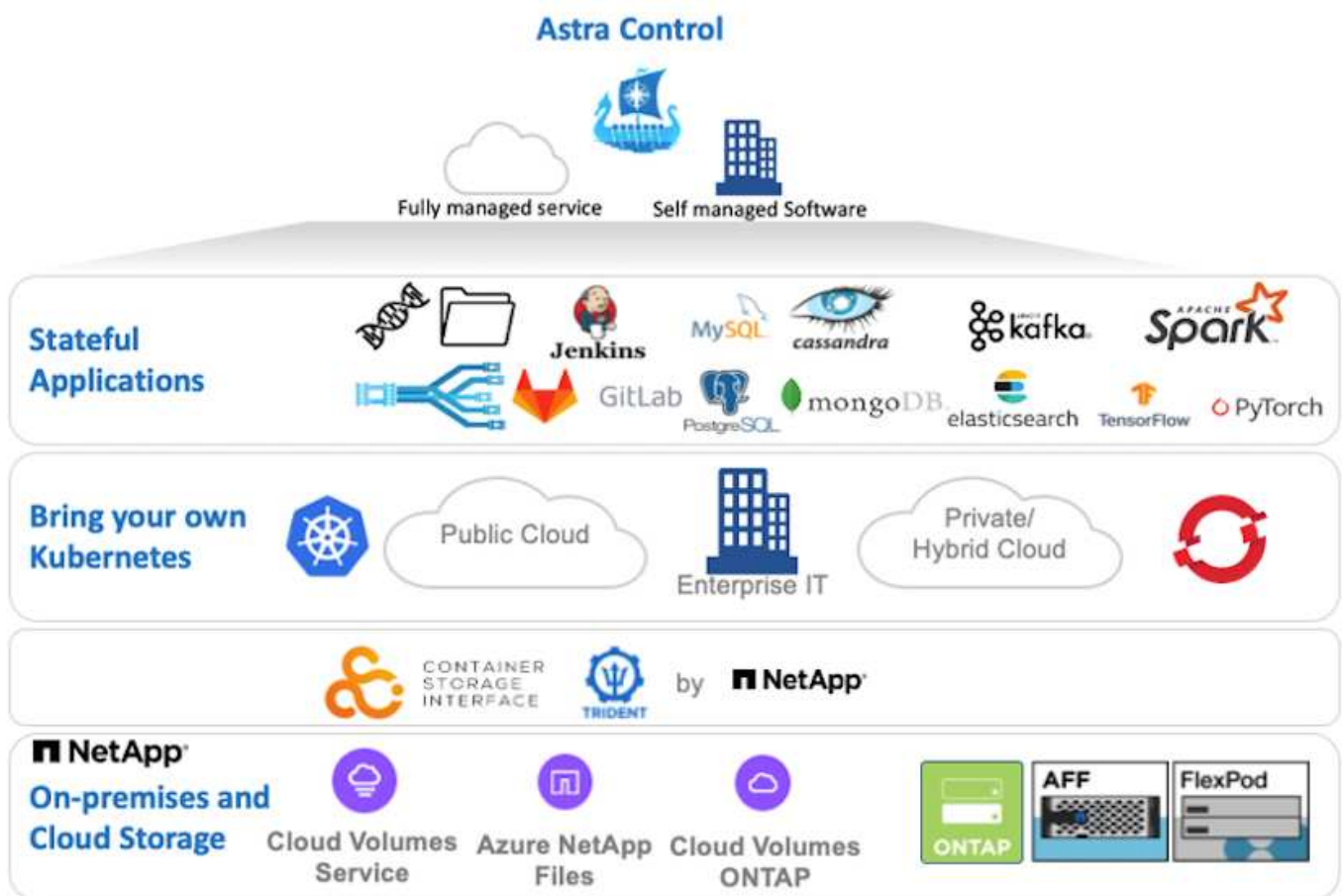
NetApp Astra Trident es un orquestador de almacenamiento de código abierto y totalmente compatible para contenedores y distribuciones de Kubernetes como Red Hat OpenShift, Rancher, VMware Tanzu etc. Si quiere más información, visite el sitio web de Astra Trident ["aquí"](#).

En las siguientes páginas se ofrece información adicional sobre los productos de NetApp que se han validado para la administración del almacenamiento persistente y de aplicaciones en la solución DevOps with NetApp:

- ["Centro de control de Astra de NetApp"](#)
- ["Astra Trident de NetApp"](#)

Descripción general de Astra Control de NetApp

Astra Control Center de NetApp ofrece un amplio conjunto de servicios de gestión de datos para aplicaciones y almacenamiento para cargas de trabajo con estado de Kubernetes puestas en marcha en un entorno local con la tecnología de protección de datos de NetApp.



NetApp Astra Control Center se puede instalar en un clúster de Kubernetes que tenga el orquestador de almacenamiento Astra Trident puesto en marcha y configurado con clases de almacenamiento y back-ends en los sistemas de almacenamiento ONTAP de NetApp.

Si desea obtener más información sobre Astra Trident, consulte ["este documento aquí"](#).

En un entorno conectado a la nube, Astra Control Center utiliza Cloud Insights para proporcionar supervisión y telemetría avanzadas. Ante la ausencia de una conexión con Cloud Insights, la supervisión y la telemetría limitadas (en siete días de métricas) están disponibles y se exportan a herramientas de supervisión nativas de Kubernetes (Prometheus y Grafana) mediante extremos de métricas abiertos.

Astra Control Center está totalmente integrado en el ecosistema de AutoSupport y Active IQ de NetApp para proporcionar soporte a los usuarios y proporcionar asistencia para la solución de problemas y mostrar las estadísticas de uso.

Además de la versión pagada de Astra Control Center, también hay disponible una licencia de evaluación de 90 días. La versión de evaluación se admite a través del correo electrónico y el canal de Slack de la comunidad. Los clientes tienen acceso a estos recursos, a otros artículos de la base de conocimientos y a la documentación disponible en la consola de soporte del producto.

Para obtener más información sobre la cartera de Astra, visite ["Sitio web de Astra"](#).

Para obtener una guía de instalación y funcionamiento detallada de Astra Control Center, siga la documentación ["aquí"](#).

Automatización de Astra Control Center

Astra Control Center tiene una API DE REST totalmente funcional para el acceso a la programación. Los usuarios pueden utilizar cualquier lenguaje de programación o utilidad para interactuar con los extremos de la API REST de Astra Control. Para obtener más información acerca de esta API, consulte la documentación de ["aquí"](#).

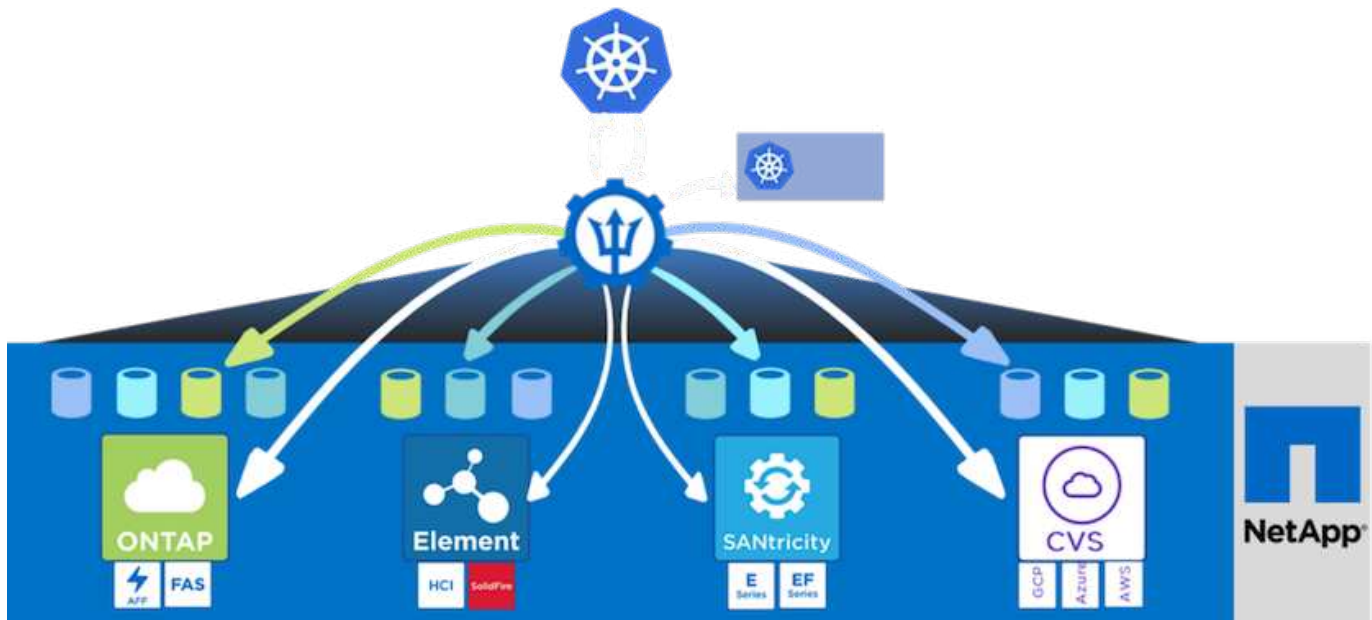
Si busca un kit de herramientas de desarrollo de software listo para usar con las API REST de Astra Control, NetApp le proporciona un kit de herramientas con Astra Control Python SDK, que puede descargar ["aquí"](#).

Si la programación no es una corrección adecuada para su situación y le gustaría utilizar una herramienta de gestión de configuración, puede clonar y ejecutar los libros de estrategia de Ansible que publica NetApp ["aquí"](#).

Descripción general de Astra Trident

Astra Trident es un orquestador de almacenamiento de código abierto y totalmente compatible para contenedores y distribuciones de Kubernetes como Red Hat OpenShift, VMware Tanzu, Anthos by Google Cloud, Rancher etc. Trident funciona con toda la cartera de almacenamiento de NetApp, incluidos los sistemas de almacenamiento ONTAP y Element de NetApp, y también admite conexiones NFS e iSCSI. Trident acelera el flujo de trabajo de DevOps al permitir que los usuarios finales aprovisionen y gestionen el almacenamiento desde sus sistemas de almacenamiento de NetApp sin necesidad de intervención del administrador de almacenamiento.

Un administrador puede configurar varios back-ends de almacenamiento a partir de necesidades de proyectos y modelos de sistema de almacenamiento que permiten funciones de almacenamiento avanzadas, como compresión, tipos de disco específicos o niveles de calidad de servicio que garantizan un cierto nivel de rendimiento. Una vez definidas estos back-ends pueden ser utilizados por los desarrolladores en sus proyectos para crear reclamaciones de volumen persistente (RVP) y conectar almacenamiento persistente a sus contenedores bajo demanda.



Astra Trident tiene un rápido ciclo de desarrollo y, al igual que Kubernetes, se publica cuatro veces al año.

La última versión de Astra Trident se lanzó en abril de 2022 en 22.04. Existe una matriz de compatibilidad con la versión de Trident probada en la que se puede encontrar la distribución de Kubernetes ["aquí"](#).

A partir del lanzamiento de la versión 20.04, el operador de Trident realiza la configuración de Trident. El operador facilita las puestas en marcha a gran escala y ofrece soporte adicional, incluida la reparación automática de pods que se implementan como parte de la instalación de Trident.

Con la versión 21.01, se puso a disposición un gráfico Helm para facilitar la instalación del operador Trident.

Consulte la documentación ["aquí"](#) Para instalar y usar Astra Trident.

Validación de casos prácticos: DevOps con NetApp Astra

Se han validado los siguientes casos de uso para DevOps con NetApp Astra:

- ["Integrar la protección en canalizaciones CI/CD con Astra Control de NetApp"](#)
- ["Aproveche Astra Control para facilitar el análisis post mortem y la restauración de la aplicación"](#)
- ["Aceleración del desarrollo de software con FlexClones de NetApp"](#)

Integrar la protección en canalizaciones CI/CD con Astra Control de NetApp

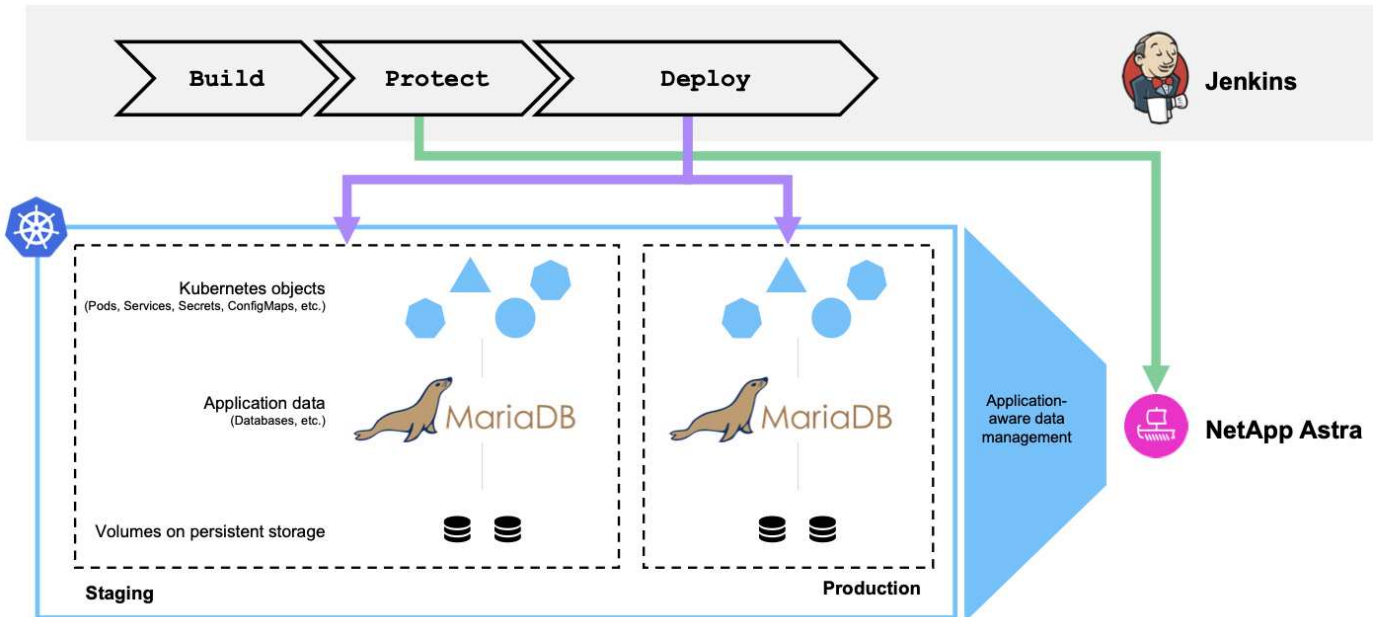
Descripción general

Uno de los usos más comunes de los flujos de trabajo de DevOps es la integración continua y las canalizaciones de implementación continua (CI/CD) que crean, integran y ejecutan suites de pruebas automatizadas en aplicaciones, mientras los desarrolladores aplican nuevo código. Los ingenieros de DevOps y los ingenieros de fiabilidad del sitio (SRE, "Site-reliability engineer") suelen tener canalizaciones dedicadas a los distintos flujos de trabajo para el desarrollo de nuevas funciones, las pruebas de regresión, las correcciones de errores, la ingeniería de calidad y otras funciones del proceso de desarrollo.

A medida que los equipos aumentan su nivel de automatización, el ritmo de los cambios de las aplicaciones en producción puede resultar abrumador. Por lo tanto, algunos equipos prefieren proteger los servicios o las

aplicaciones de producción. Además de proteger las imágenes de código y contenedor, también quieren proteger el estado de la aplicación, los datos de configuración (como objetos y recursos de Kubernetes asociados con la aplicación) y los datos persistentes de una aplicación.

En este caso de uso, analizamos con detalle una canalización de promoción a producción que pone en marcha una nueva versión de una aplicación: Primero, a un entorno de almacenamiento provisional y, finalmente, a un entorno de producción. Este ejemplo se aplica de igual forma a los principales clouds públicos y también a un entorno local. Aunque mostramos el despliegue de una versión de la aplicación, la canalización también se puede utilizar con otras estrategias, como la implementación azul/verde o canaria. Como parte de la canalización de CI/CD, vamos a proteger la aplicación creando una copia de seguridad completa de la aplicación. Un backup coherente con las aplicaciones de la aplicación de producción y sus datos, estado y configuración pueden ser útiles para numerosos flujos de trabajo de DevOps.



Se utilizó la aplicación para validar este caso de uso "**Magento**", Una solución de comercio electrónico con un front-end basado en la web; una instancia de Elasticsearch para las funciones de búsqueda y análisis; y una base de datos MariaDB que realiza un seguimiento de todos los detalles del inventario de compras y las transacciones. Esta aplicación en contenedor se instaló en un clúster de Red Hat OpenShift. Cada pod de la aplicación usaba volúmenes persistentes para almacenar datos. Los volúmenes persistentes fueron creados automáticamente por NetApp Astra Trident, el orquestador de almacenamiento compatible con Container Storage Interface para Kubernetes que permite aprovisionar el almacenamiento en los sistemas de almacenamiento de NetApp. Además, para utilizar las funcionalidades de protección de aplicaciones de Astra Control Center, Astra Control gestiona esta aplicación, que se utiliza para activar los backups de aplicaciones que almacenaban el estado de la aplicación y los datos contenidos en volúmenes persistentes. Utilizamos la "**Kit de desarrollo de software Astra Control Python de NetApp**" Para automatizar el proceso de activación de backups de aplicaciones, que posteriormente se introdujo en una canalización de CI/CD. Esta canalización se creó y ejecutó utilizando una herramienta de CI/CD conocida llamada [**Jenkins**] para automatizar el flujo para crear, proteger e implementar la aplicación.

Repasemos los requisitos previos y el procedimiento para introducir la protección en una canalización CI/CD.

Requisitos previos de validación de casos de uso

Se pusieron en marcha y configuraron como requisitos previos las siguientes herramientas o plataformas:

1. OpenShift Container Platform de Red Hat

2. Astra Trident de NetApp instalado en OpenShift con un back-end al sistema ONTAP de NetApp configurado
3. Se configuró un storagegrid predeterminado, que apunta al back-end ONTAP de NetApp
4. NetApp Astra Control Center instalado en un clúster OpenShift
5. OpenShift Cluster se ha agregado como un clúster gestionado a Astra Control Center
6. Jenkins se ha instalado en un clúster de OpenShift y se ha configurado con un nodo de agente con un motor Docker instalado en él

Instalación de la aplicación

Comencemos por la instalación inicial de la aplicación en los entornos de configuración y producción. Para este caso de uso, este paso es un requisito previo, por lo que se realiza de forma manual. La canalización de CI/CD se utiliza para los flujos de trabajo posteriores de creación e implementación como resultado de las versiones nuevas de la aplicación.

El entorno de producción en este caso de uso es un espacio de nombres llamado `magento-prod` y el entorno de ensayo correspondiente es un espacio de nombres denominado `magento-staging` Configurado en el clúster de Red Hat OpenShift. Para aplicar la aplicación, realice los siguientes pasos:

1. Instale la aplicación Magento mediante el gráfico de timón de bitnami en el entorno de producción. Utilizamos RWX PVs para las vainas Magento y MariaDB.

```
[netapp-user@rhel7 na_astra_control_suite]$ helm install --version 14
magento bitnami/magento -n magento-prod --create-namespace --set
image.tag=2.4.1-debian-10-
r11,magentoHost=10.63.172.243,persistence.magento.accessMode=ReadWriteMa
ny,persistence.apache.accessMode=ReadWriteMany,mariadb.master.persistenc
e.accessModes[0]=ReadWriteMany
```



La tabla de timón de Magento bitnami requiere un servicio LoadBalancer para exponer el servicio de GUI de Magento. Nosotros usamos "[MetalLB](#)" para proporcionar un servicio de equilibrador de carga en las instalaciones en este ejemplo.

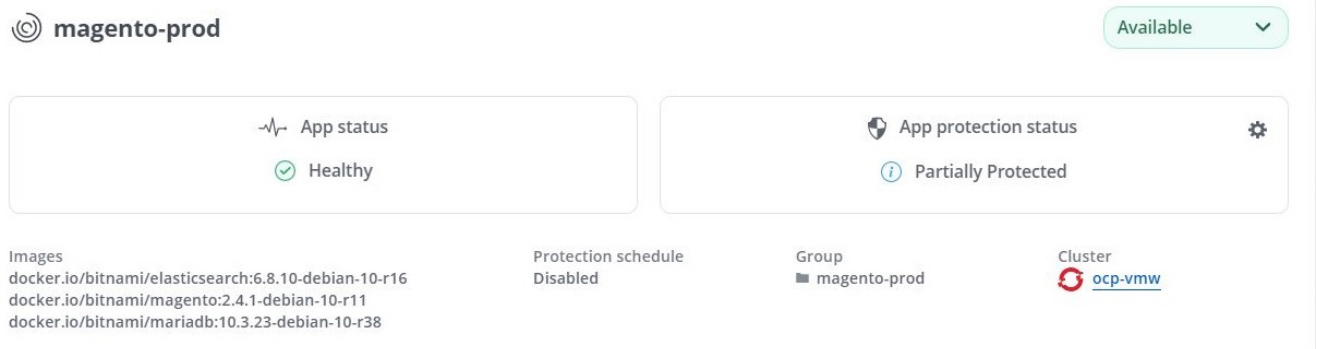
2. Después de unos minutos, verifique que estén en ejecución todos los pods y servicios.

```
[netapp-user@rhel7 na_astra_control_suite]$ oc get pods -n magento-prod
NAME                                                    READY   STATUS
RESTARTS      AGE
magento-9d658fd96-grxmt                                1/1     Running
0              49m
magento-elasticsearch-coordinating-only-69869cc5-768rm 1/1     Running
0              49m
magento-elasticsearch-data-0                            1/1     Running
0              49m
magento-elasticsearch-master-0                         1/1     Running
0              49m
magento-mariadb-0                                       1/1     Running
0              49m
```

3. Repita el mismo procedimiento para el entorno de ensayo.

Gestione la aplicación Magento en Astra Control Center

1. Desplácese a aplicaciones y seleccione la ficha aplicaciones detectadas.
2. Haga clic en los puntos suspensivos con la aplicación Magento en el entorno de producción (magento-prod) Y haga clic en Administrar.
3. La aplicación Magento es ahora gestionada por Astra Control Center. Todas las operaciones compatibles con Astra Control se pueden realizar en la aplicación. Anote también la versión de la aplicación.



magento-prod Available

App status: Healthy

App protection status: Partially Protected

Images: docker.io/bitnami/elasticsearch:6.8.10-debian-10-r16, docker.io/bitnami/magento:2.4.1-debian-10-r11, docker.io/bitnami/mariadb:10.3.23-debian-10-r38

Protection schedule: Disabled

Group: magento-prod

Cluster: ocp-vmw

4. Repita los pasos para administrar la aplicación Magento en el entorno de ensayo (magento-staging).

Canalización de CI/CD con protección integrada

Cuando trabajamos con nuevas versiones de aplicaciones, utilizamos una canalización CI/CD para construir la imagen de contenedor, realizar backups tanto de los entornos de ensayo como de producción, implementar la nueva versión de la aplicación en el entorno de ensayo, esperar la aprobación de la promoción a la producción, a continuación, implemente la nueva versión de la aplicación en el entorno de producción. Para utilizar una canalización de CI/CD, lleve a cabo los siguientes pasos:

1. Inicie sesión en Jenkins y cree las credenciales necesarias: Una para Magento creds, una para MariaDB admin creds y la tercera para MariaDB root creds.
2. Desplácese hasta Manage Jenkins > Manage Credentials y haga clic en el dominio adecuado.

3. Haga clic en Agregar credenciales y establezca el tipo en Nombre de usuario con contraseña y ámbito establecido en Global. Introduzca el nombre de usuario, la contraseña y el ID para las credenciales y haga clic en OK.

Dashboard > Credentials > System > Global credentials (unrestricted)

Back to credential domains

Add Credentials

Kind: Username with password

Scope: Global (Jenkins, nodes, items, all child items, etc)

Username: admin

☐ Treat username as secret

Password:

ID: magento-cred

Description:

OK

4. Repita el mismo procedimiento para las otras dos credenciales.
5. Vuelva a la consola, cree una canalización haciendo clic en Nuevo elemento y, a continuación, haga clic en canalización.
6. Copie la canalización del archivo Jenkinsfile "aquí".
7. Pegue la canalización en la sección de canalización Jenkins y, a continuación, haga clic en Guardar.
8. Rellene los parámetros de la canalización Jenkins con los detalles respectivos, incluida la versión del gráfico del timón, la versión de la aplicación Magento a la que se va a actualizar, la versión del kit de herramientas de Astra, el FQDN de Astra Control Center, el token de API y su ID de instancia. Especifique el registro docker, el espacio de nombres y Magento IP tanto de los entornos de producción como de ensayo, y también especifique los identificadores de credenciales de las credenciales creadas.

```
MAGENTO_VERSION = '2.4.1-debian-10-r14'
CHART_VERSION = '14'
RELEASE_TYPE = 'MINOR'
ASTRA_TOOLKIT_VERSION = '2.0.2'
ASTRA_API_TOKEN = 'xxxxxxxxx'
ASTRA_INSTANCE_ID = 'xxx-xxx-xxx-xxx-xxx'
ASTRA_FQDN = 'netapp-astra-control-center.org.example.com'
DOCKER_REGISTRY = 'docker.io/netapp-solutions-cicd'
PROD_NAMESPACE = 'magento-prod'
PROD_MAGENTO_IP = 'x.x.x.x'
STAGING_NAMESPACE = 'magento-staging'
STAGING_MAGENTO_IP = 'x.x.x.x'
MAGENTO_CREDS = credentials('magento-cred')
MAGENTO_MARIADB_CREDS = credentials('magento-mariadb-cred')
MAGENTO_MARIADB_ROOT_CREDS = credentials('magento-mariadb-root-cred')
```

9. Haga clic en Crear ahora. La canalización comienza a ejecutarse y avanza a lo largo de los pasos. La imagen de la aplicación se crea primero y se carga en el registro del contenedor.

Build & Publish Segment	Build Docker Image	Publish Image to Registry	Protect & Deploy Segment	Install & Configure Pre-requisites	Download & Configure Astra Toolkit	Backup Tasks	Backup of Staging Env	Backup of Production Env	Deploy to Staging environment [Minor/Patch]	Deploy to Staging environment [Major]	Promote to Production?	Deploy to Production environment [Minor/Patch]	Deploy to Production environment [Major]	Delete temporary files
4s	24s	5s	213ms	40s	2s	290ms	1min 38s	1min 2s	6min 29s	229ms	361ms	2min 57s	200ms	850ms
3s														
18min 29s														

10. Las copias de seguridad de aplicaciones se inician mediante Astra Control.

magento-prod
Available

App status
Healthy

App protection status
Partially Protected

Images

Protection schedule

Group

Cluster

docker.io/bitnami/elasticsearch:6.8.10-debian-10-r16

Disabled

magento-prod

ocp-vmw

docker.io/bitnami/magento:2.4.1-debian-10-r11

docker.io/bitnami/mariadb:10.3.23-debian-10-r38


Overview
Data protection
Storage
Resources
Activity


Actions
Configure protection policy
Search


1-8 of 8 entries

<input type="checkbox"/>	Name	Ready	On-Schedule/On-Demand	Created ↑	Actions
<input type="checkbox"/>	upgrade-prod-2-4-1-debian-10-r20		On-Demand	2021/10/29 14:43 UTC	Running

11. Una vez que las fases de copia de seguridad se hayan completado correctamente, compruebe las copias de seguridad desde Astra Control Center.


magento-prod
Available



App status
Healthy


App protection status
Partially Protected

Images
 docker.io/bitnami/elasticsearch:6.8.10-debian-10-r16
 docker.io/bitnami/magento:2.4.1-debian-10-r11
 docker.io/bitnami/mariadb:10.3.23-debian-10-r38



Protection schedule
 Disabled

Group
 magento-prod

Cluster
 ocp-vmw

Overview
Data protection
Storage
Resources
Activity

Actions
 Configure protection policy

Search
 


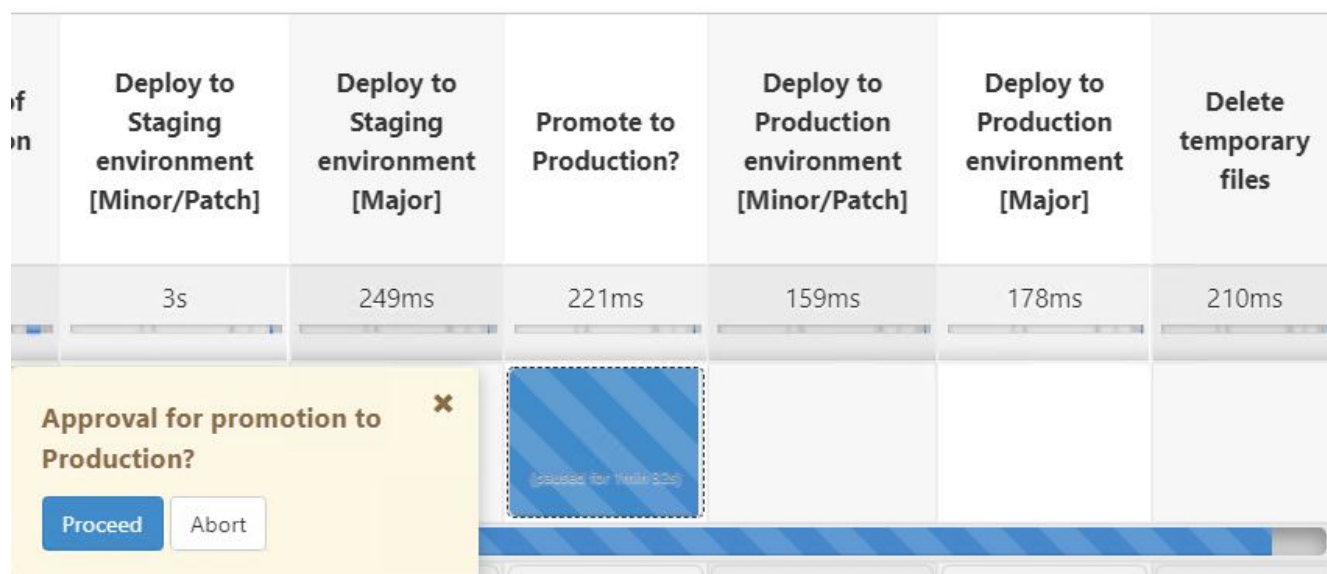
1–8 of 8 entries
 <
>

<input type="checkbox"/>	Name	Ready	On-Schedule/On-Demand	Created ↑	Actions
<input type="checkbox"/>	upgrade-prod-2-4-1-debian-10-r20	Healthy	On-Demand	2021/10/29 14:43 UTC	Available

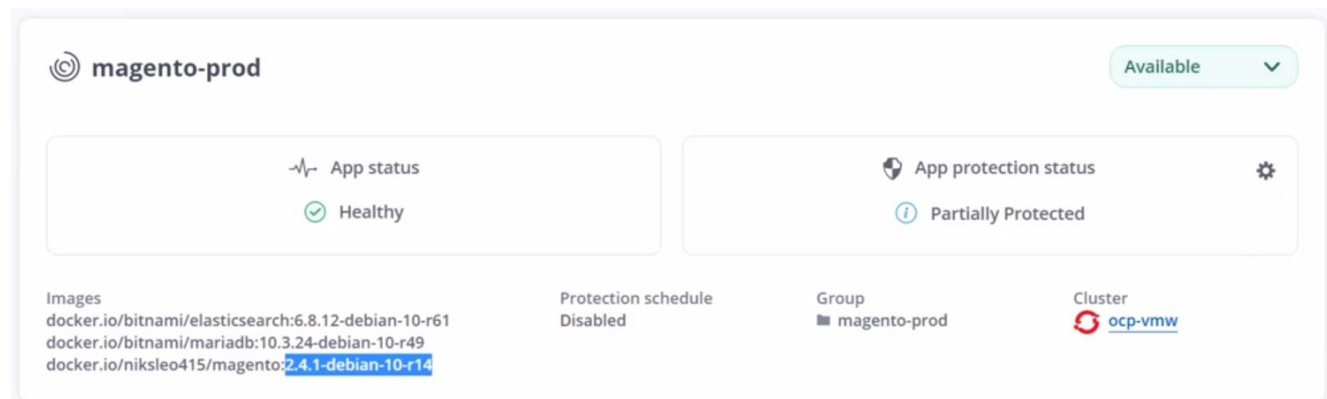
12. A continuación, la nueva versión de la aplicación se implementa en el entorno de almacenamiento provisional.

Build & Publish Segment	Build Docker Image	Publish Image to Registry	Protect & Deploy Segment	Install & Configure Pre-requisites	Download & Configure Astra Toolkit	Backup Tasks	Backup of Staging Env	Backup of Production Env	Deploy to Staging environment [Minor/Patch]	Deploy to Staging environment [Major]	Promote to Production?	Deploy to Production environment [Minor/Patch]	Deploy to Production environment [Major]	Delete temporary files
4s	47s	7s	238ms	1min 25s	2s	273ms	1min 53s	1min 18s	5min 20s	211ms	337ms	2min 39s	187ms	780ms
3s	4min 16s	30s	485ms	7s	3s	153ms	6min 9s	5min 9s						
7min 1s														

13. Una vez completado este paso, el programa espera a que el usuario apruebe la implementación a producción. En esta fase, suponga que el equipo de QA realiza algunas pruebas manuales y aprueba la producción. A continuación, puede hacer clic en aprobar para implementar la nueva versión de la aplicación en el entorno de producción.



14. Compruebe que la aplicación de producción también se ha actualizado a la versión deseada.



Como parte de la canalización CI/CD, demostramos la capacidad para proteger la aplicación creando un backup completo compatible con aplicaciones. Dado que se ha realizado un backup de toda la aplicación como parte de la canalización de promoción a producción, puede sentirse más seguro de las puestas en marcha de aplicaciones altamente automatizadas. Este backup consciente de la aplicación que contiene los datos, el estado y la configuración de la aplicación puede ser útil para numerosos flujos de trabajo de DevOps. Un flujo de trabajo importante sería volver a la versión anterior de la aplicación en caso de problemas imprevistos.

Aunque demostramos un flujo de trabajo CI/CD a través de la herramienta Jenkins, este concepto se puede extrapolar de forma sencilla y eficiente a distintas herramientas y estrategias. Para ver este caso de uso en acción, vea el vídeo ["aquí"](#).

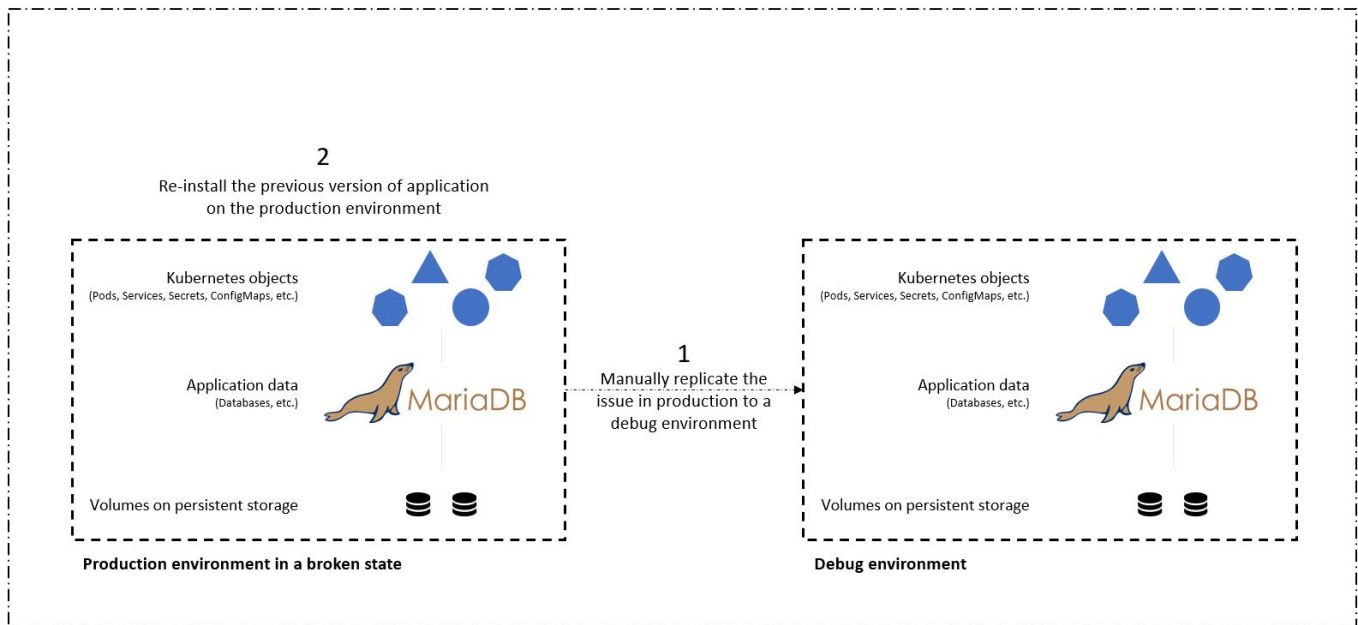
Utilice Astra Control para facilitar el análisis post mortem y restaurar la aplicación

Descripción general

En la ["primer caso de uso"](#), Demostramos cómo usar Astra Control Center de NetApp para proteger sus aplicaciones en Kubernetes. En esa sección se describe cómo integrar los backups de aplicaciones a través de Astra Control directamente en su flujo de trabajo de desarrollo gracias al SDK de Python del kit de herramientas Astra de NetApp. Este enfoque permite la protección de los entornos de desarrollo y producción

mediante la automatización de backups bajo demanda durante el proceso de integración continua y de implementación continua (CI/CD). Con esta capa adicional de protección de datos consistente con las aplicaciones añadida a la canalización CI/CD y a las aplicaciones de producción, los procesos de desarrollo son seguros si algo sale mal en el proceso, lo que promueve buenas prácticas de continuidad del negocio.

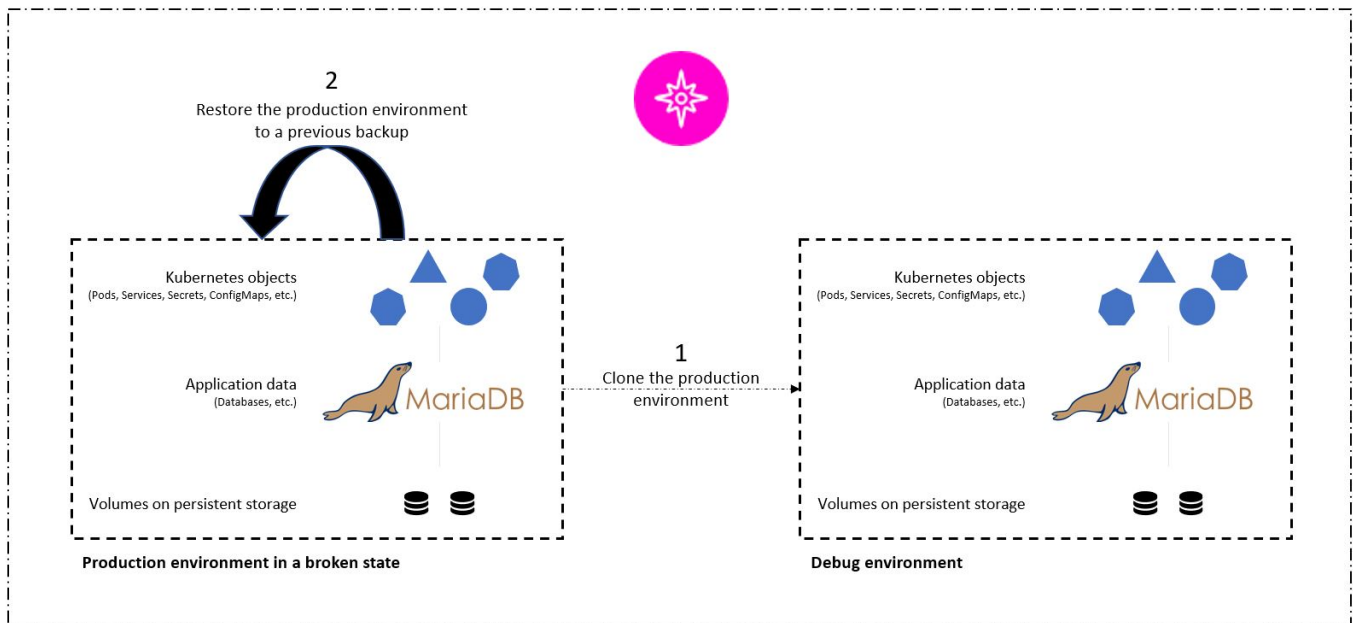
En un flujo de trabajo tradicional, después de haber encontrado un error cuando la aplicación se actualiza a una nueva versión, el equipo de desarrollo intentaría solucionar el problema en tiempo real a partir de los informes de errores que proporcionaban los clientes. Como alternativa, en el primer signo de problema, el equipo podría intentar volver a implementar la aplicación en un entorno de depuración paralelo para desconectar ese proceso. Podrían volver a poner en marcha una base de código anterior de una versión anterior a la producción, lo que restauraría la aplicación a la orden de trabajo.



Aunque este enfoque funciona, el equipo tendría que asegurarse de que el estado de la aplicación de producción rota coincide con el de la versión que se ve en producción cuando se produjeron los problemas. También tendrían que dedicar tiempo a la promoción de la producción de funcionalidad comprobada obteniendo código desde su repositorio y volviendo a poner en marcha las imágenes de la máquina para restaurar la aplicación a un estado en buen funcionamiento. Asimismo, en este escenario no se tuvo en cuenta si el código defectuoso corrompía la base de datos de producción en sí. Lo ideal es que existan procesos de backup independientes para los datos de la base de datos, pero, ¿debemos asumir que son coherentes con el estado de la aplicación tal como se publicó? Aquí es donde las ventajas de los backups con estado y consistentes con las aplicaciones, las restauraciones y los clones con Astra Control realmente muestran su valor.

En primer lugar, podemos utilizar Astra Control para facilitar el análisis post mortem sobre el estado de la aplicación. Para ello, clonamos la versión de producción con buggy en un entorno de prueba paralelo con la aplicación. Tener este entorno separado en su estado de bugs-plot nos permite solucionar el problema en tiempo real.

Además, Astra Control admite la función de restauración in situ que nos permite restaurar la aplicación de producción a una última copia de seguridad aceptable (que precedió a la versión afligida del código). La versión restaurada asume la posición de la aplicación de producción de buggy anterior, de manera coherente con la aplicación y con estado, incluida la IP de entrada asignada previamente. Por lo tanto, los clientes que acceden al interfaz de usuario no tendrían conocimiento de la transición a la versión de backup.



Requisitos previos de validación de casos de uso

Se pusieron en marcha y configuraron como requisitos previos las siguientes herramientas o plataformas:

- OpenShift Container Platform de Red Hat.
- Astra Trident de NetApp instalado en OpenShift con un back-end configurado para un sistema ONTAP de NetApp.
- Se configuró un storagegrid predeterminado, que apunta al back-end ONTAP de NetApp.
- NetApp Astra Control Center instalado en un clúster OpenShift.
- OpenShift Cluster se ha agregado como un clúster gestionado a Astra Control Center.
- Jenkins se ha instalado en un clúster de OpenShift.
- Aplicación Magento instalada en el entorno de producción. El entorno de producción en este caso de uso es un espacio de nombres llamado "evento-prod" en un clúster de Red Hat OpenShift.
- Aplicación de producción gestionada por Astra Control Center.
- Backup(s) de funcionalidad comprobada de la aplicación de producción capturada con Astra Control.

Clonar y restaurar la canalización

Teniendo en cuenta que la aplicación se ha actualizado a una nueva versión, la aplicación del entorno de producción (magento-prod) no se comporta como se pretende después de la actualización. Supongamos que los datos que devuelven las consultas de interfaz de usuario no coinciden con la solicitud o que la base de datos se ha dañado de hecho. Para clonar y restaurar la canalización, siga estos pasos:



This site can't be reached

10.63.172.243 took too long to respond.

Try:

- Checking the connection
- [Checking the proxy and the firewall](#)
- [Running Windows Network Diagnostics](#)

ERR_CONNECTION_TIMED_OUT

Reload

Details

1. Inicie sesión en Jenkins y cree una canalización haciendo clic en Nuevo elemento y, a continuación, en canalización.
2. Copie la canalización del archivo Jenkinsfile ["aquí"](#).
3. Pegue la canalización en la sección de canalización Jenkins y, a continuación, haga clic en Guardar.
4. Rellene los parámetros de la canalización Jenkins con los detalles respectivos, como la versión actual de la aplicación Magento en producción, el FQDN de Astra Control Center, el token de API, el ID de instancia y el nombre de aplicación o el espacio de nombres de los entornos de producción y depuración, y los nombres de los clústeres de origen y destino. Para este caso de uso, el entorno de producción es un espacio de nombres denominado "evento-prod" y el entorno de depuración es un espacio de nombres denominado "depuración" configurado en un clúster de Red Hat OpenShift.

```
MAGENTO_VERSION = '2.4.1-debian-10-r14'
ASTRA_TOOLKIT_VERSION = '2.0.2'
ASTRA_API_TOKEN = 'xxxxxx'
ASTRA_INSTANCE_ID = 'xxx-xxx-xxx-xxx-xxx'
ASTRA_FQDN = 'netapp-astra-control-center.org.example.com'
PROD_APP_NAME = 'magento-prod'
DEBUG_APP_NAME = 'magento-debug'
DEBUG_NAMESPACE = 'magento-debug'
PROD_KUBERNETES_CLUSTER = 'ocp-vmw'
DEBUG_KUBERNETES_CLUSTER = 'ocp-vmw'
```

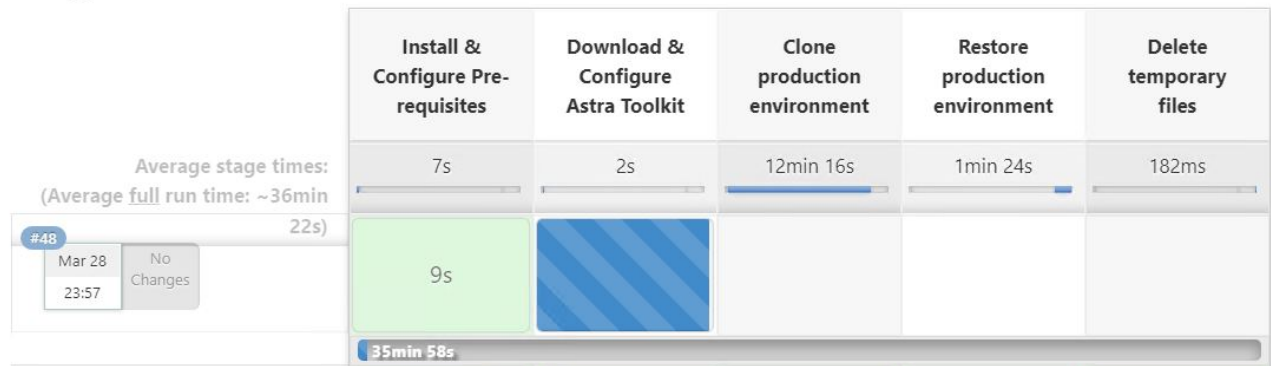
5. Haga clic en Crear ahora. La canalización comienza a ejecutarse y avanza a lo largo de los pasos. La aplicación se clona primero en el estado actual en un entorno de depuración y, a continuación, se restaura a un backup de trabajo conocido.

Pipeline magento_clone-for-triage_restore-from-backup

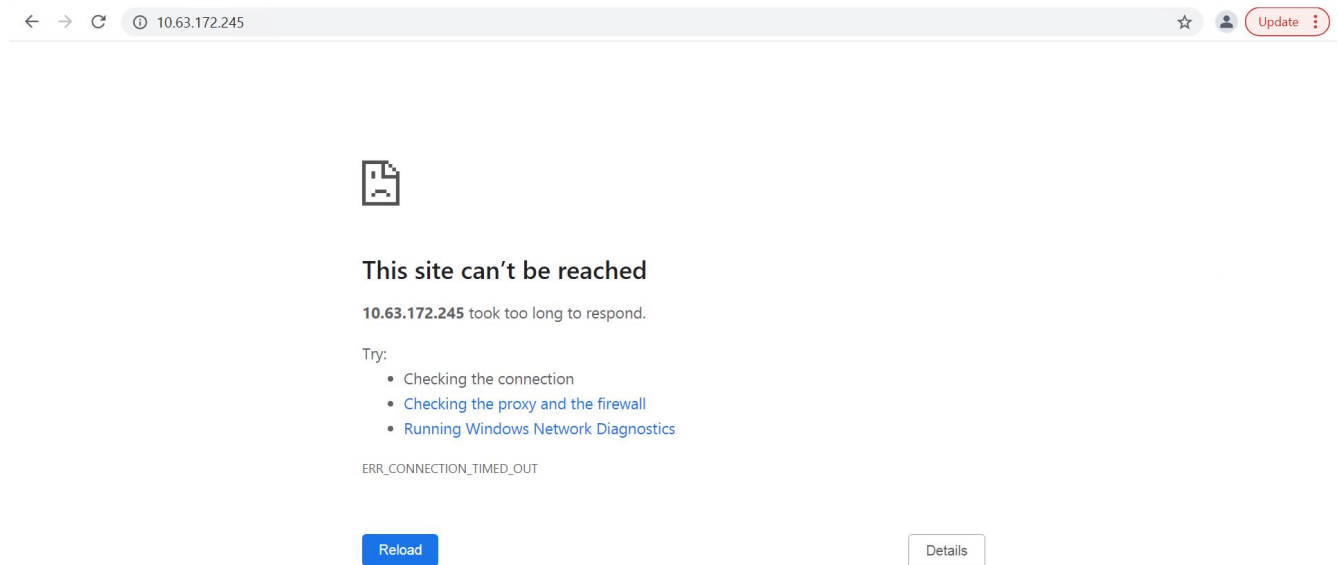


Recent Changes

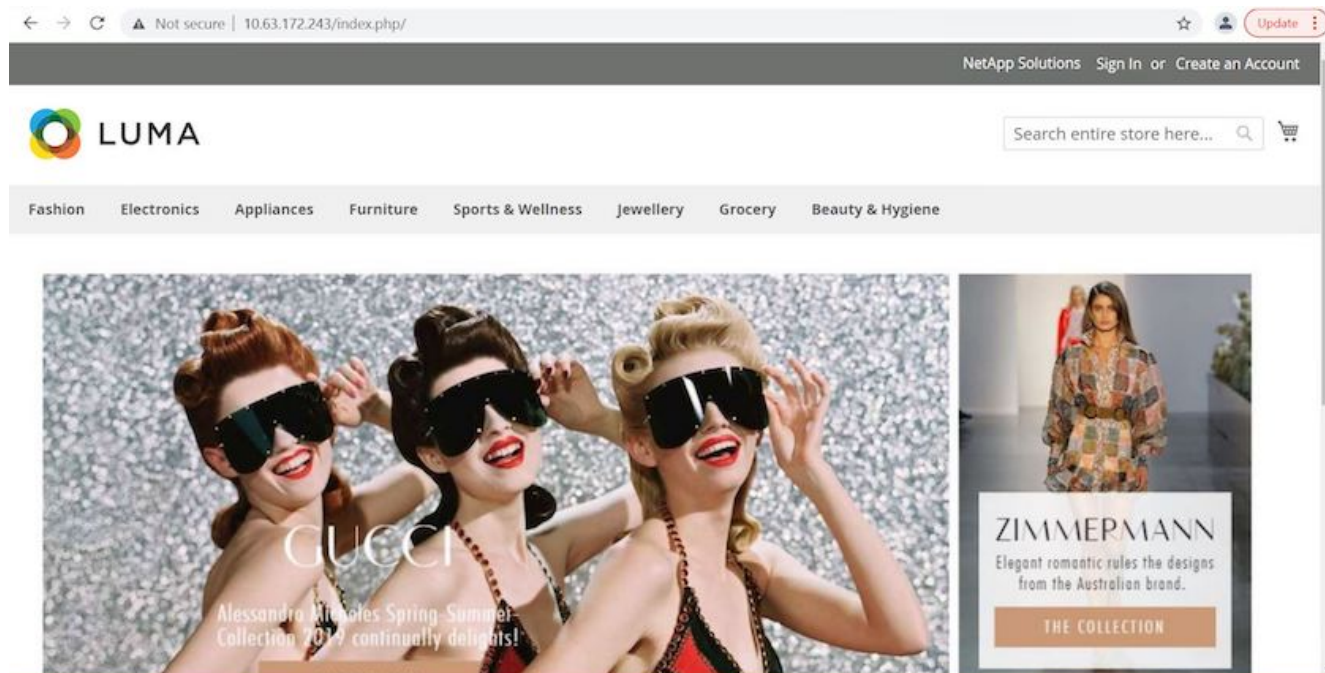
Stage View



6. Compruebe que la aplicación clonada sea la versión que contiene errores.



7. Comprobar que el entorno de producción se ha restaurado en un backup en funcionamiento y que la aplicación en producción funciona de la forma esperada.



Estas dos operaciones en tándem aceleran el retorno a las operaciones empresariales normales. Para ver este caso de uso en acción, vea el vídeo "[aquí](#)".

Acelere el desarrollo de software con la tecnología FlexClone de NetApp

Descripción general

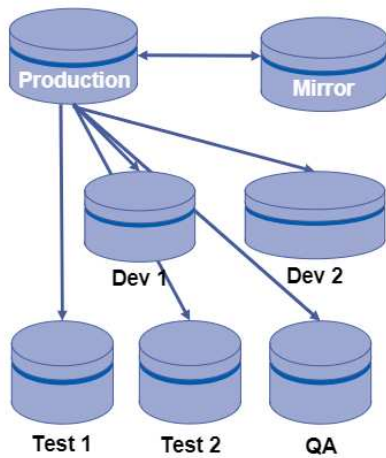
El clonado de una aplicación puesta en marcha en un clúster de Kubernetes es una herramienta muy útil para los desarrolladores que desean acelerar sus flujos de trabajo al compartir entornos con partners o probar nuevas versiones de código en un entorno de desarrollo sin interferir con la versión en la que trabajan actualmente. El clonado con estado y consistente con las aplicaciones de una aplicación Kubernetes es una de las principales funciones que se incluyen en Astra Control de NetApp, junto con el backup y la restauración de aplicaciones. Si una aplicación se clona en el mismo clúster de Kubernetes con el mismo back-end de almacenamiento, Astra Control utiliza de forma predeterminada la tecnología FlexClone de NetApp para la deduplicación de volúmenes de datos persistentes, lo que acelera considerablemente el proceso. Al acelerar este proceso, el entorno clonado se aprovisiona y está disponible para su uso en pocos momentos, lo que permite a los desarrolladores reanudar su trabajo con una breve pausa en comparación con la nueva puesta en marcha de su entorno de pruebas o desarrollo. Además, para una mayor comodidad, todas las funciones disponibles en Astra Control de NetApp se pueden llamar con una API, que permite una integración sencilla en marcos de automatización como Ansible. Por lo tanto, los entornos se pueden almacenar en niveles incluso más rápido porque solo se necesitan cambios menores en un libro de aplicaciones o un rol para comenzar el procedimiento de clonación.

¿Qué es la tecnología FlexClone de NetApp?

La tecnología FlexClone de NetApp es una copia editable, basada en copias Snapshot de un momento específico de un FlexVol de NetApp. Se aprovisionan casi al instante, contienen todos los datos del volumen de origen y no consumen espacio de almacenamiento adicional hasta que los datos del nuevo volumen empiecen a desviarse del origen. A menudo se utilizan en entornos basados en desarrollo o en plantillas cuando varias copias de datos son útiles para fines de configuración y los sistemas de almacenamiento tienen recursos limitados para aprovisionar estos volúmenes. En comparación con un sistema de almacenamiento tradicional en el que los datos deben copiarse varias veces, por lo que se consume un tiempo y un espacio de almacenamiento considerable, la tecnología FlexClone de NetApp acelera las tareas dependientes del

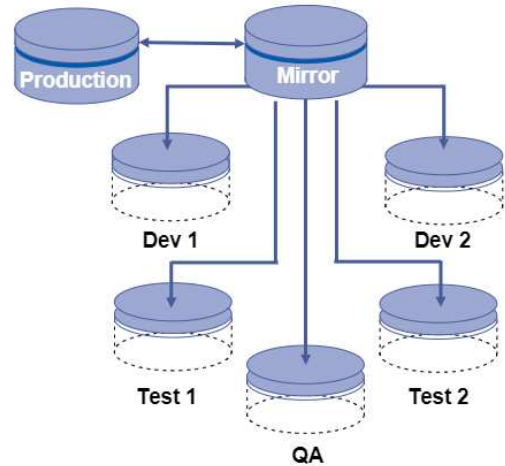
almacenamiento.

Traditional Data Copies



Traditional physical copies take additional time and consume additional storage space

NetApp FlexClone Copies



NetApp FlexClone copies are near instantaneous and only consume space when written to

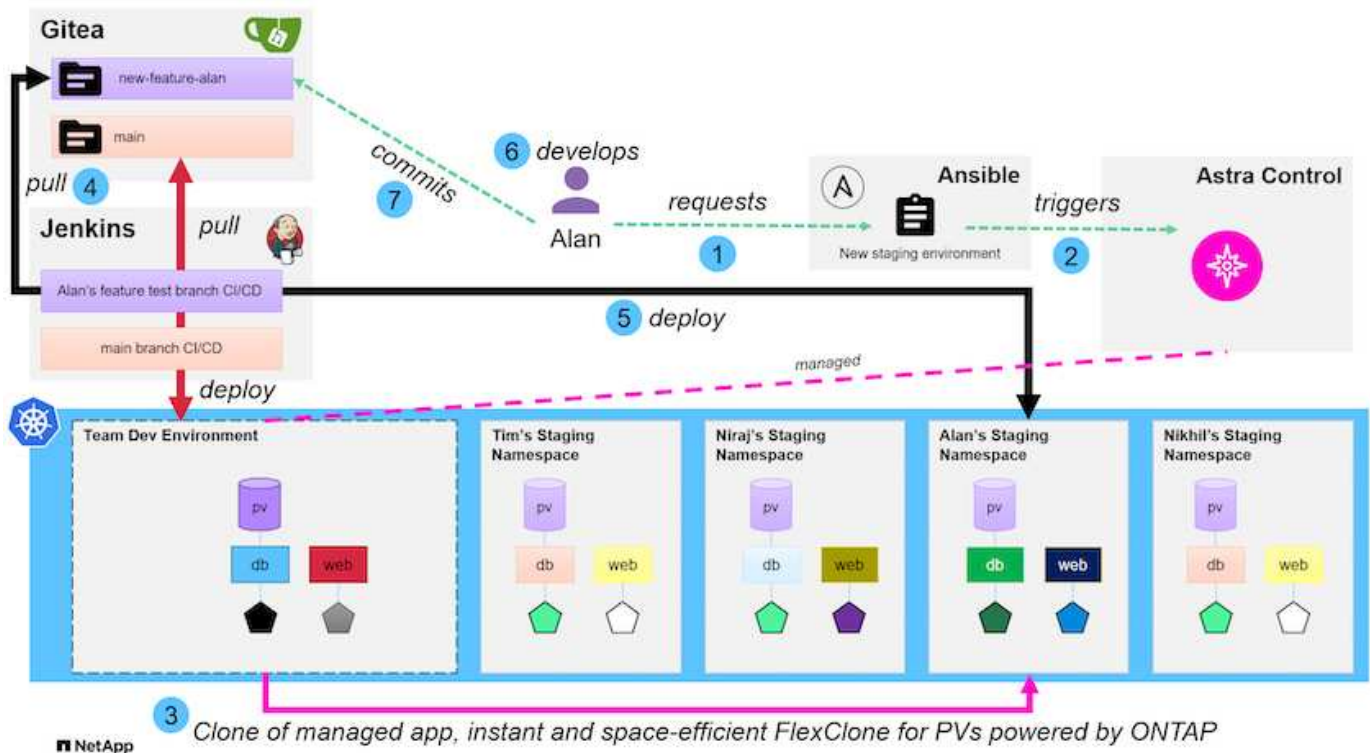
Si quiere más información sobre la tecnología FlexClone de NetApp, visite la página en "[Documentos de NetApp](#)".

Requisitos previos

1. Una distribución de Kubernetes compatible, como Red Hat OpenShift 4.6.8 o posterior, Rancher 2.5 o Kubernetes 1.19 o posterior.
2. NetApp Astra Control Center 21.12+.
3. Un sistema ONTAP de NetApp con un back-end de almacenamiento configurado mediante la Astra Trident de NetApp.
4. Ansible 2.9 o posterior.
5. Plantillas para los entornos que le gustaría clonar como aplicaciones gestionadas en Astra Control de NetApp.

Introducción a casos de uso

Para este caso de uso, visualizamos algo similar al siguiente flujo de trabajo:



1. Un usuario ejecuta el libro de estrategia de Ansible para crear un nuevo entorno de almacenamiento provisional.
2. Ansible utiliza el módulo URI-API para llamar a Astra Control y ejecutar la operación de clonado.
3. Astra Control ejecuta una operación de clonación en un entorno de plantilla preaprovisionado, creando así una nueva aplicación administrada.



Este entorno puede ser una única aplicación independiente en desarrollo o en todo un entorno de desarrollo, como una canalización CI/CD de Jenkins.

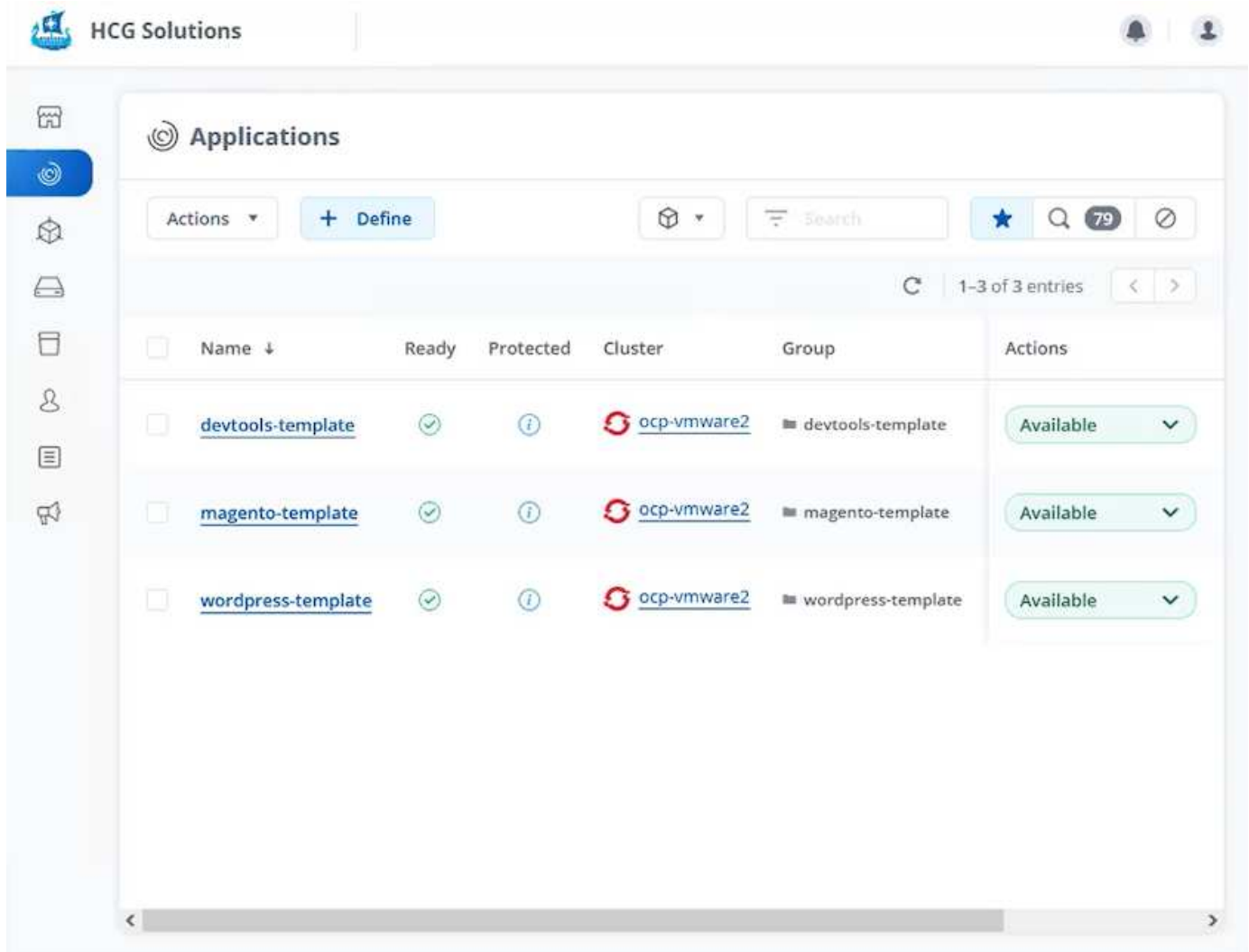
4. A continuación, el usuario extrae una versión de su código al entorno de desarrollo clonado desde un repositorio en línea como Gitea.
5. La nueva versión de la aplicación se pone en marcha y gestiona con Astra Control de NetApp.



Estos dos procesos se pueden automatizar.

6. El usuario puede desarrollar código nuevo en este entorno clonado.
7. Cuando el usuario está satisfecho con sus esfuerzos de desarrollo, puede devolver el código al repositorio alojado.

El caso de uso que se presenta aquí depende de la existencia de plantillas maestras para los entornos o aplicaciones concretas que desee clonar. En nuestro entorno hemos creado tres de estas plantillas, una para la implementación de Wordpress, otra para la implementación de Magento y otra para un entorno CI/CD de Jenkins con Gitea que hemos titulado DevTools.



Cada uno de estos entornos se gestiona mediante Astra Control de NetApp, con volúmenes persistentes que se almacenan actualmente en un sistema de almacenamiento ONTAP de NetApp con un back-end NFS proporcionado por Astra Trident de NetApp.

Validación de casos de uso

1. Clone el kit de herramientas de Ansible que proporciona el equipo de ingeniería de soluciones de NetApp, que incluye el rol de clonado y el libro de estrategia de actualización de aplicaciones.

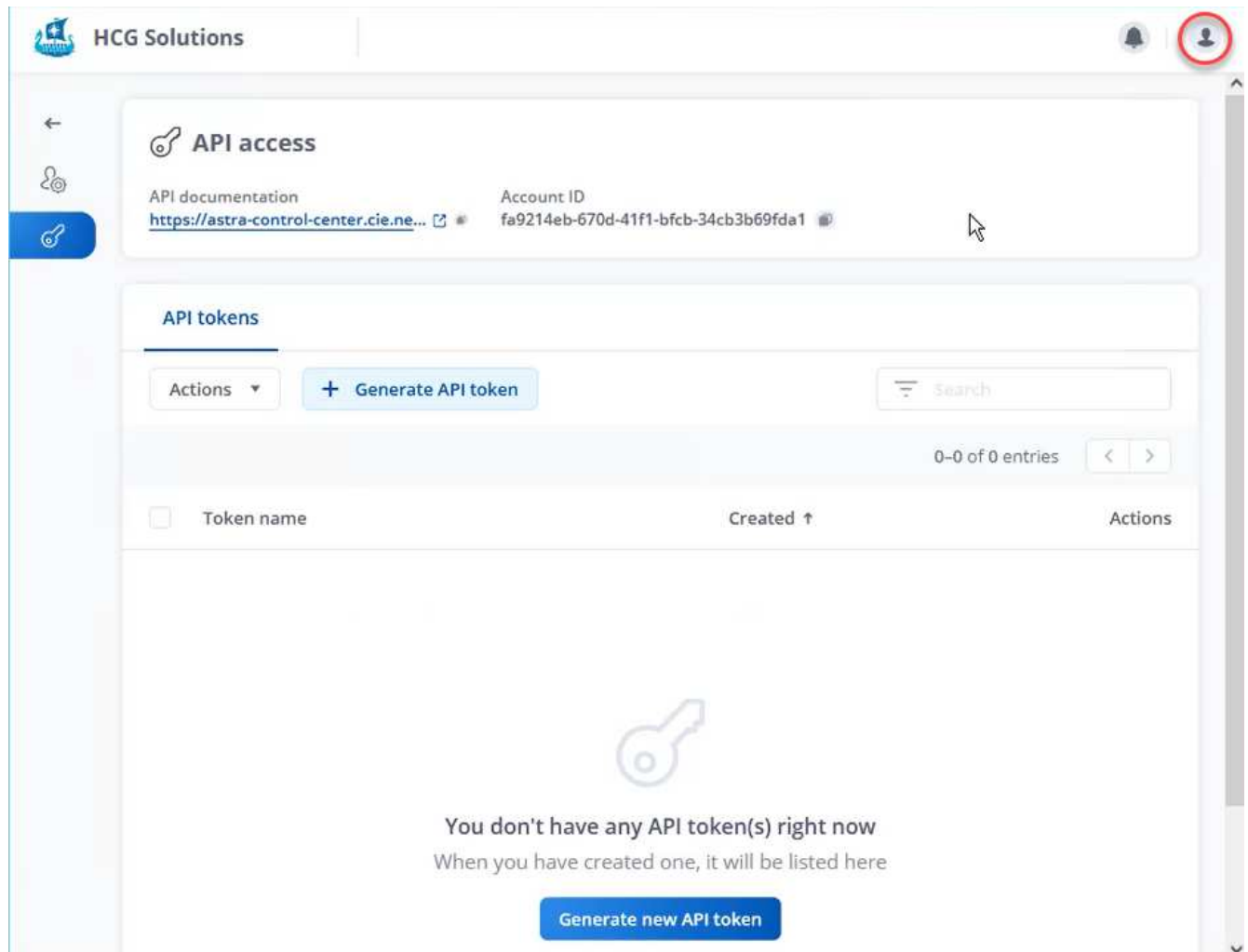
```
[netapp-user@rhel7 ~]$ git clone https://github.com/NetApp-Automation/na_astra_control_suite.git
[netapp-user@rhel7 ~]$ cd na_astra_control_suite
```

2. Editar `vars/clone_vars.yml` Y rellene los valores globales que se ajusten a su entorno de Astra Control.

```
astra_control_fqdn: astra-control-center.example.com
astra_control_account_id: "xxxx-xxxx-xxxx-xxxx-xxxx"
astra_control_api_token: "xxxxx"
```



Los valores del entorno global que debe rellenar están disponibles en el icono de perfil de usuario de NetApp Astra Control, en el menú API Access.



- Una vez completadas las variables globales, puede elegir los valores de la aplicación específica que desea clonar. Para clonar el entorno devtools a un entorno personal llamado alan-devtools, haría lo siguiente:

```
clone_details:
- clone_name: alan-devtools
  destination_namespace: alan-dev-namespace
  source_cluster_name: ocp-vmware2
  destination_cluster_name: ocp-vmware2
  source_application_name: devtools-template
```



Para aprovechar la tecnología FlexClone de NetApp en el proceso de clonación, `src-cluster` y `dest-cluster` debe ser igual.

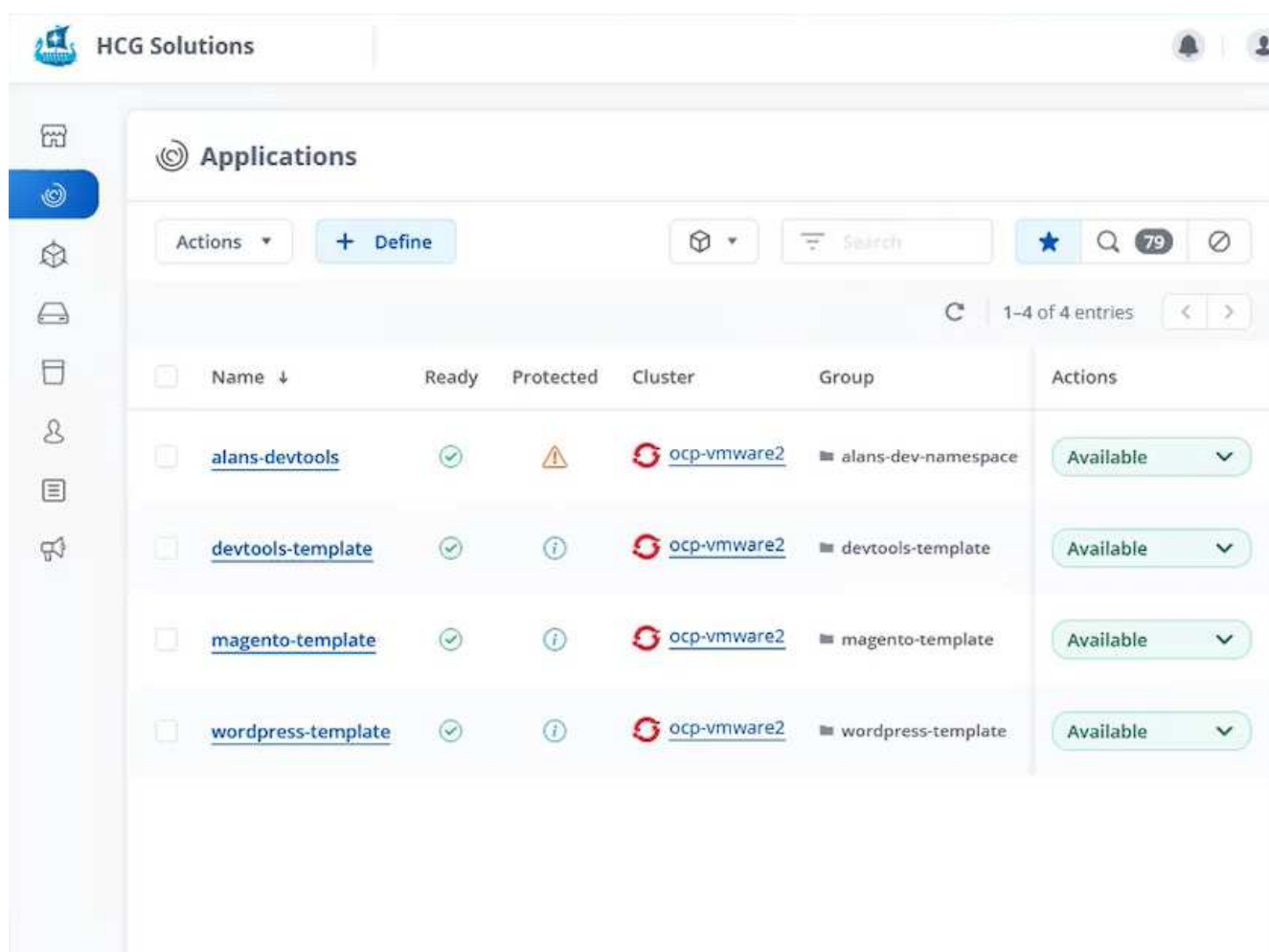
- Ahora puede ejecutar el libro de aplicaciones para clonar la aplicación.

```
[netapp-user@rhel7 na_astra_control_suite]$ ansible-playbook -K clone_app_playbook.yml]
```



el libro de aplicaciones como escrito debe ser ejecutado por el usuario raíz o por alguien que pueda escalar a través del proceso sudo pasando el argumento "-K".

- Una vez que el libro de aplicaciones complete su ejecución, la aplicación clonada aparecerá como disponible en la consola del Centro de control de Astra.



- A continuación, un usuario puede iniciar sesión en el entorno Kubernetes en el que se ha puesto en marcha la aplicación, comprobar que la aplicación está expuesta con una nueva dirección IP e iniciar el trabajo de desarrollo.

Para ver una demostración de este caso práctico y un ejemplo de cómo actualizar una aplicación, consulte ["aquí"](#).

Vídeos y demostraciones: DevOps con NetApp Astra

En los siguientes vídeos se muestran algunas de las funcionalidades descritas en este documento:

[Protección de datos en canalización CI/CD con Astra Control Center](#)

[Aproveche Astra Control de NetApp para realizar un análisis post-mortem y restaurar su aplicación](#)

[Acelere el desarrollo de software con Astra Control y la tecnología FlexClone de NetApp](#)

Información adicional: DevOps con NetApp Astra

Si quiere más información sobre la información descrita en este documento, consulte los siguientes sitios web:

- Documentación de NetApp

["https://docs.netapp.com/"](https://docs.netapp.com/)

- Documentación de Astra Trident

["https://docs.netapp.com/us-en/trident/"](https://docs.netapp.com/us-en/trident/)

- Documentación del centro de control Astra de NetApp

["https://docs.netapp.com/us-en/astra-control-center/"](https://docs.netapp.com/us-en/astra-control-center/)

- Documentación de Ansible

["https://docs.ansible.com/"](https://docs.ansible.com/)

- Documentación de Red Hat OpenShift

["https://access.redhat.com/documentation/en-us/openshift_container_platform/4.8/"](https://access.redhat.com/documentation/en-us/openshift_container_platform/4.8/)

- Documentación de rancher

["https://rancher.com/docs/"](https://rancher.com/docs/)

- Documentación de Kubernetes

["https://kubernetes.io/docs/home/"](https://kubernetes.io/docs/home/)

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.