Le DevOps avec NetApp Astra

NetApp Solutions

NetApp
April 18, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/netapp-solutions/containers/dwn_overview_devops.html on April 18, 2024. Always check docs.netapp.com for the latest.

Sommaire

Tr-4919 : le DevOps avec NetApp Astra . . . 1
Cas d’utilisation . . . 1
Valeur commerciale . . . 1
Présentation de la technologie . . . 1
Présentation du DevOps . . . 2
Présentation des systèmes de stockage NetApp . . . 4
Présentation de l’intégration du stockage NetApp . . . 8
Validation du cas d’utilisation : le DevOps avec NetApp Astra . . . 11
Vidéos et démonstrations : le DevOps avec NetApp Astra . . . 28
NetApp Astra, avec le DevOps . . . 29

Tr-4919 : le DevOps avec NetApp Astra

Alan Cowles et Nikhil M Kulkarni, NetApp

Cas d’utilisation

L’architecture du DevOps avec NetApp Astra vise à offrir un niveau de valeur exceptionnel à ses clients dans plusieurs cas :

- Déployez et gérez facilement des applications et des environnements de développement déployés sur les distributions Kubernetes prises en charge.
- Discussion sur des cas d’utilisation réels pour les workflows DevOps et exemples d’outils et de méthodes que NetApp peut proposer pour faciliter l’adoption et l’utilisation de ces méthodes.
- Exploration de la façon dont les snapshots, les sauvegardes et les clones cohérents au niveau des applications peuvent être utilisés pour améliorer l’expérience DevOps.

Valeur commerciale

Les entreprises se tournent de plus en plus vers les pratiques DevOps pour créer de nouveaux produits, réduire les cycles de lancement et ajouter rapidement de nouvelles fonctionnalités. En raison de leur nature inné et agile, les conteneurs et les microservices ont un rôle essentiel dans l’accompagnement des pratiques DevOps. Cependant, la pratique du DevOps à l’échelle de production dans un environnement d’entreprise présente ses propres défis et impose certaines exigences à l’infrastructure sous-jacente, notamment :

- La haute disponibilité à tous les niveaux de la pile afin que les flux de travail ne soient jamais interrompus.
- La facilité de déploiement et de gestion des procédures pour l’utilisateur final.
- Une infrastructure programmable et basée sur des API pour suivre le rythme des microservices et de l’agilité pour les développeurs.
- Possibilité de faire évoluer l’infrastructure de manière indépendante et automatisée en fonction des besoins des workloads
- Outre la protection des applications parallèlement à leurs datasets persistants de sauvegarde pour les workflows DevOps, les délais de mise sur le marché sont réduits, car la priorité n’est pas donnée à la redéploiement ou à la copie manuelle des données.

Compte tenu de ces fonctionnalités et de ces défis, ce rapport technique décrit le processus d’amélioration et de simplification des cas d’utilisation du DevOps pour les applications conteneurisées à l’aide du vaste portefeuille de produits NetApp.

Présentation de la technologie

La solution DevOps avec NetApp comprend plusieurs composants principaux :

Pratiques DevOps

Les pratiques DevOps se concentrent sur des opérations automatisées, reproductibles et facilement gérables qui améliorent le workflow de développement en permettant aux utilisateurs de contrôler l’environnement dans lequel ils développent leur code. Cette solution offre plusieurs exemples et cas d’utilisation pour lesquels la technologie NetApp peut bénéficier de ce type d’opérations.

Orchestration de conteneurs

De nombreuses plateformes d'orchestration de conteneurs sont actuellement utilisées. Bien que la plupart de ces plateformes reposent sur Kubernetes, les avantages et les inconvénients des deux plateformes sont chacun. Il est donc important de comprendre les ensembles de fonctionnalités et les intégrations lors de la sélection d'une plateforme d'orchestration de conteneurs pour les workflows DevOps. Avec la suite de produits NetApp Astra, nous prenons en charge les plateformes suivantes pour des cas d'utilisation complets du DevOps :

- "Red Hat OpenShift" 4.6.8+
- "Rancher" 2.5+
- "Kubernetes" 1.20+
- "VMware Tanzu Kubernetes Grid" 1.4+
- "VMware Tanzu Kubernetes Grid Integrated Edition" 1.12.2+

Systèmes de stockage NetApp

NetApp propose plusieurs systèmes de stockage parfaitement adaptés aux data centers d'entreprise et aux déploiements de cloud hybride. Le portefeuille NetApp inclut des systèmes de stockage NetApp ONTAP, NetApp Element et E-Series, tous capables d'assurer un stockage persistant pour les applications conteneurisées.

Pour plus d'informations, rendez-vous sur le site Web de NetApp "ici".

Intégrations du stockage NetApp

NetApp Astra Control Center propose un ensemble complet de services de gestion du stockage et des données respectueuse des applications pour les workloads Kubernetes avec état, déployés dans un environnement sur site et optimisés par la technologie de protection des données NetApp de confiance.

Pour plus d'informations, rendez-vous sur le site Web NetApp Astra "ici".

Astra Trident est un orchestrateur de stockage open source entièrement pris en charge pour les conteneurs et les distributions Kubernetes telles que Red Hat OpenShift, VMware Tanzu, Anthos by Google Cloud etc..

Pour en savoir plus, rendez-vous sur le site Web Astra Trident "ici".

Présentation du DevOps

Au cours des dernières années, les entreprises qui créent des logiciels adoptent les concepts du DevOps. Les pratiques DevOps éliminent les obstacles organisationnels en rapprochant les équipes de développement et opérationnelles. Les pratiques DevOps permettent également aux équipes d'accélérer la livraison, d'accroître la disponibilité et de renforcer la stabilité des services et des applications, ce qui améliore la productivité de l'équipe. En outre, l'adoption d'une structure d'automatisation constitue également un élément clé de la réussite : création, test et applications d'exploitation à grande échelle ou gestion d'une plateforme ou d'une pile d'infrastructure entièrement automatisée. Vous trouverez ci-dessous quelques exemples d'utilisation principaux du DevOps dans lesquels les solutions NetApp peuvent être mises en œuvre pour améliorer les

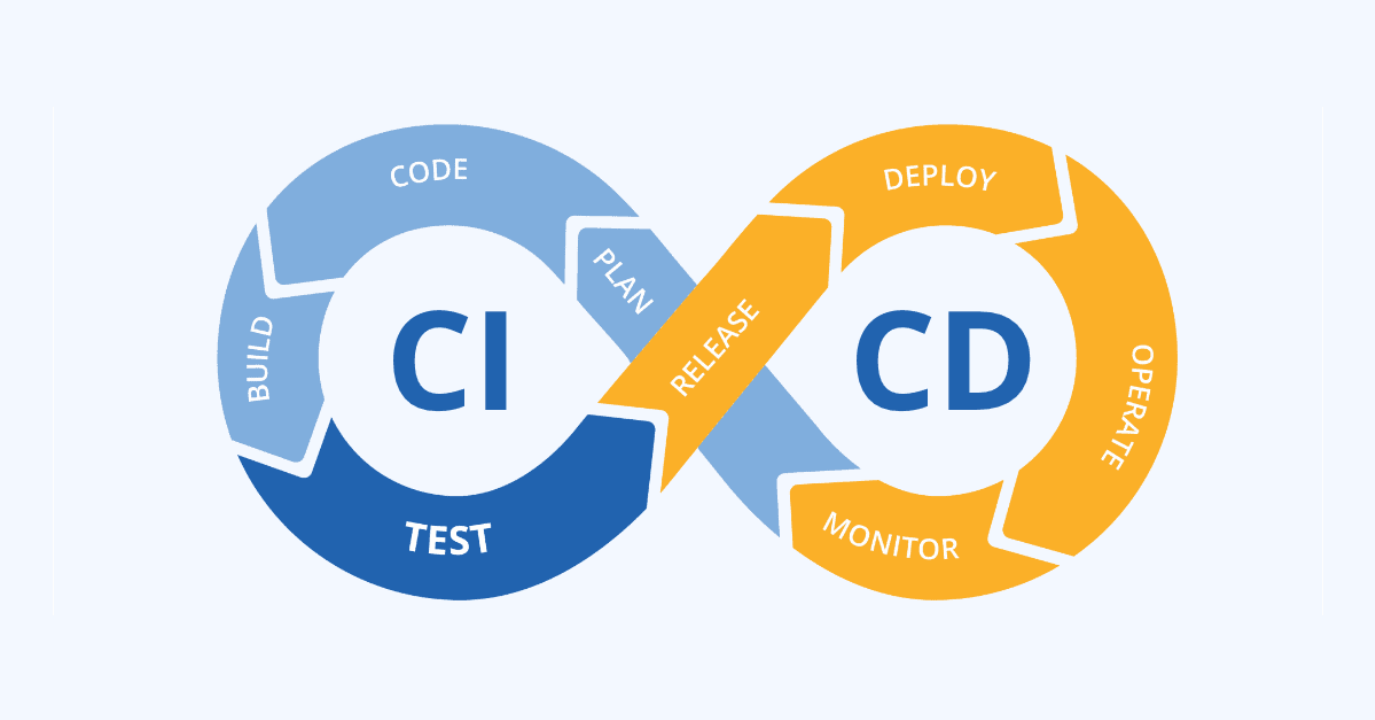
expériences des professionnels DevOps dans leurs pratiques quotidiennes.

Cas d’utilisation de DevOps

Bien que le DevOps ne soit pas défini de manière universelle, les solutions pour les praticiens DevOps contiennent généralement des constructions ou des idéologies similaires qui permettent une mise en œuvre, des répétitions et une gestion à grande échelle. Les sections suivantes décrivent les cas d’utilisation potentiels des workflows DevOps de solutions NetApp.

Intégration continue, livraison continue et déploiement continu (ci/CD)

L’intégration continue, la livraison continue et le déploiement continu (ci/CD) est une approche de codage qui encourage les développeurs à mettre en œuvre et à transformer leurs pratiques de codage en établissant une méthode qui leur permet de mettre à jour, de tester et de déployer le code de manière automatisée. La méthode la plus courante par laquelle l’intégration et la livraison continues sont implémentées dans la plupart des workflows DevOps est celle du pipeline ci/CD et plusieurs applications logicielles tierces peuvent aider à atteindre cet objectif.



Pour en savoir plus sur les workflows de type ci/CD, consultez les exemples d’applications classiques suivants :

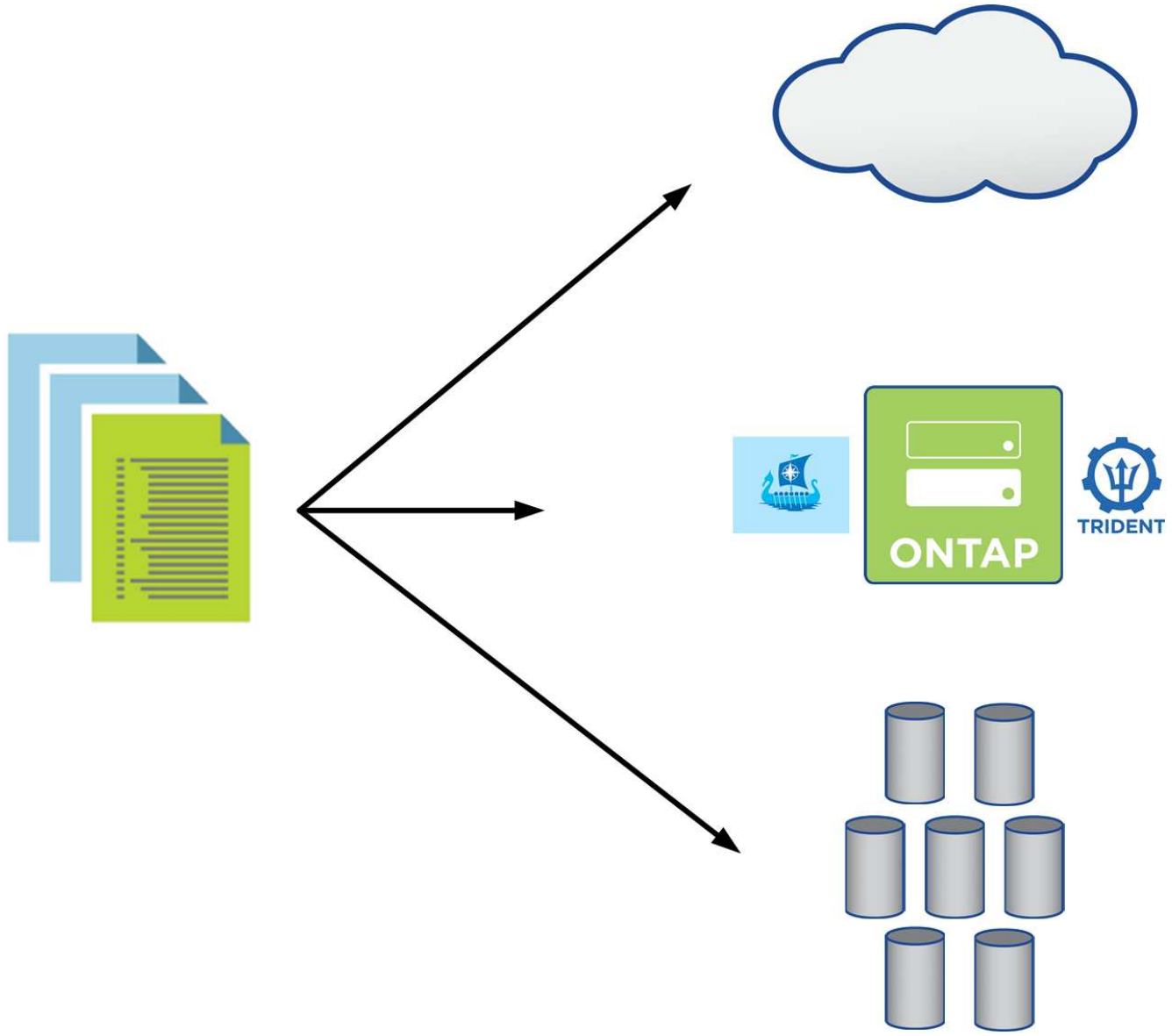
"ArgoCD"
"Jenkins"
"Tekton"

Certains des cas d’utilisation mentionnés plus loin dans ce rapport technique ont été démontrés dans Jenkins, mais les principes directeurs de l’IC/CD peuvent être appliqués à tous les outils qu’une entreprise a mis en œuvre dans ses propres pratiques.

Infrastructure-as-code

L’infrastructure-as-code permet de provisionner et de gérer les ressources IT via des commandes, des API et

des kits de développement logiciel (SDK) automatisés. Ce concept améliore considérablement l'expérience DevOps en supprimant les limitations de ressources ou de data Center physiques susceptibles d'empêcher les développeurs d'atteindre leurs objectifs.

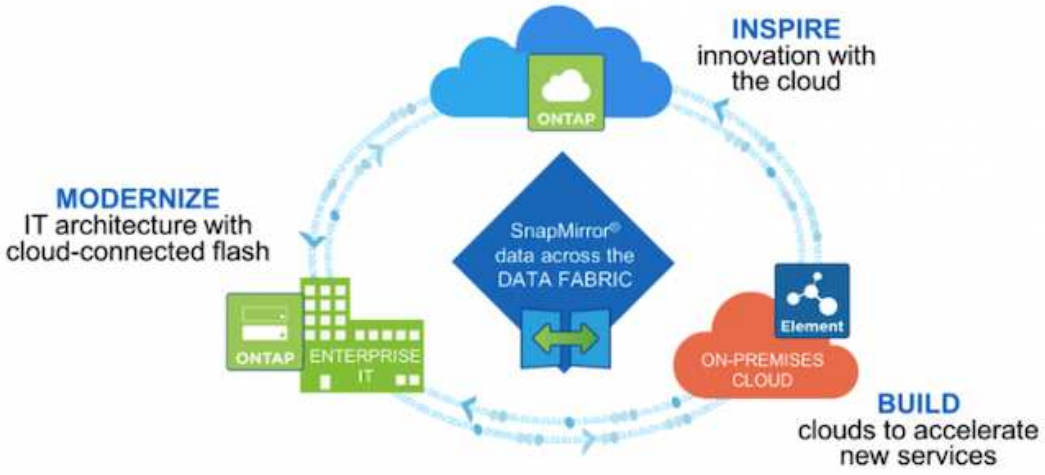


Les utilisateurs finaux utilisent souvent des langages de programmation tels que "Python" ou des outils d'automatisation tels que "Ansible" ou "Puppet" pour créer des actions automatisées et reproductibles d'évolutivité de l'infrastructure qui peuvent être appelées par les développeurs lorsque cela s'avère nécessaire.

NetApp ONTAP et Astra Control contiennent des API publiques, des modules ansible ou des kits de développement logiciel qui facilitent l'automatisation des opérations et leur intégration dans les processus DevOps.

Présentation des systèmes de stockage NetApp

NetApp propose plusieurs plateformes de stockage compatibles avec Astra Trident et Astra Control pour le provisionnement, la protection et la gestion des données pour les applications conteneurisées.



- Les systèmes AFF et FAS exécutent NetApp ONTAP et fournissent aussi bien le stockage en mode fichier (NFS) que en mode bloc (iSCSI).
- Cloud Volumes ONTAP et ONTAP Select offrent les mêmes avantages, respectivement, dans le cloud et dans l'espace virtuel.
- NetApp Cloud Volumes Service (AWS/GCP) et Azure NetApp Files proposent un stockage basé sur des fichiers dans le cloud.

> Chaque système de stockage du portefeuille NetApp simplifie la gestion et le déplacement des données entre les sites sur site et le cloud, de sorte que vos données sont là où sont vos applications.

Les pages suivantes contiennent des informations supplémentaires sur les systèmes de stockage NetApp validés dans la solution DevOps with NetApp :

- "NetApp ONTAP"

NetApp ONTAP

NetApp ONTAP est un puissant outil de gestion du stockage. Il inclut des fonctionnalités telles qu'une interface graphique intuitive, des API REST avec intégration de l'automatisation, des analyses prédictives et des actions correctives informées par IA, des mises à niveau matérielles sans interruption et des importations intersystèmes de stockage.

Pour en savoir plus sur la baie de stockage NetApp ONTAP, consultez la "Site Web NetApp ONTAP".

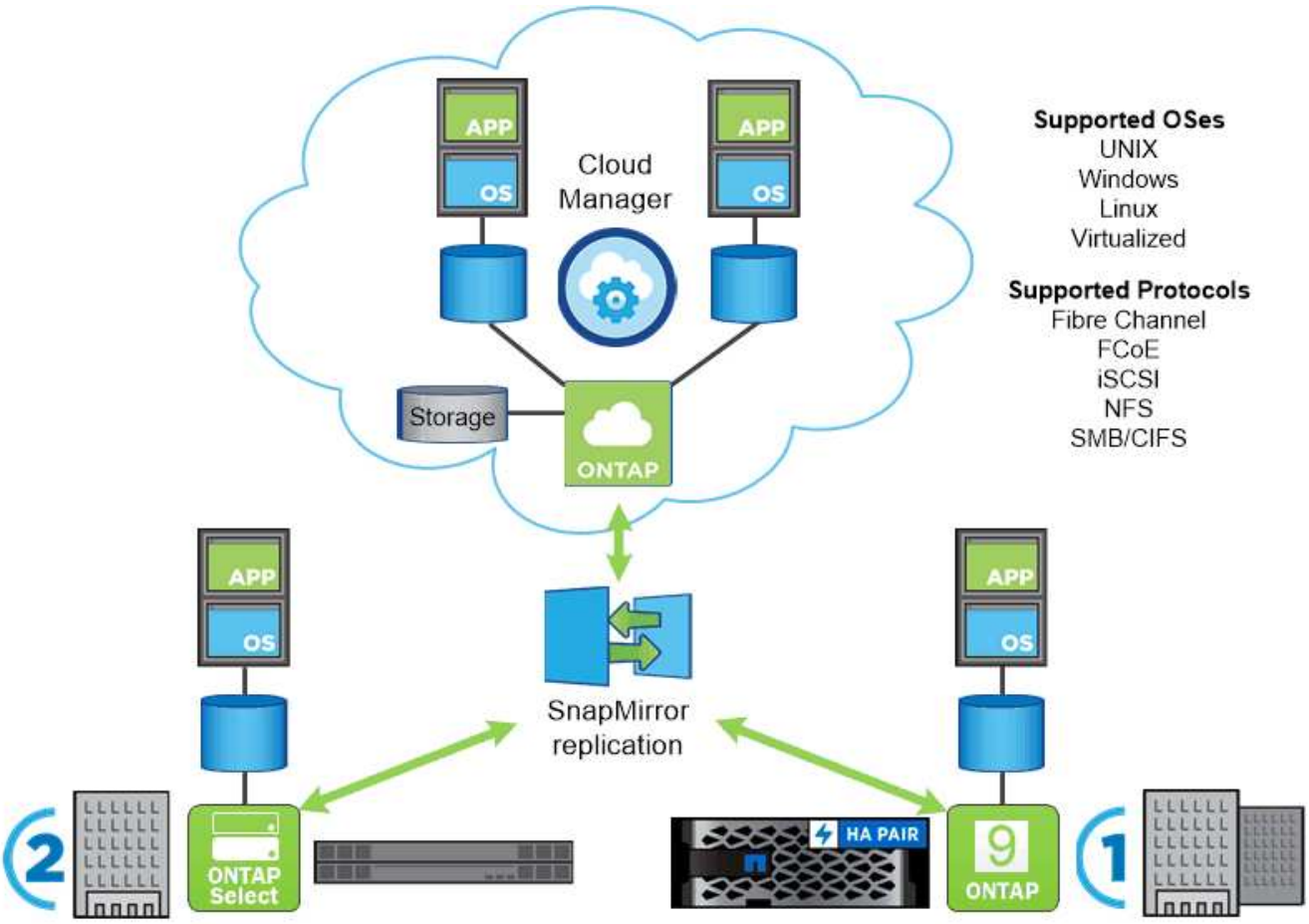
ONTAP offre les fonctionnalités suivantes :

- Système de stockage unifié avec accès et gestion simultanés aux données de NFS, CIFS, iSCSI, FC, FCoE, Et les protocoles FC-NVMe.

- Différents modèles de déploiement incluent des configurations matérielles sur site 100 % Flash, hybrides et 100 % HDD, des plateformes de stockage basées sur des VM sur un hyperviseur pris en charge comme ONTAP Select, et dans le cloud comme Cloud Volumes ONTAP.
- Amélioration de l'efficacité du stockage des données sur les systèmes ONTAP avec la prise en charge du Tiering automatique des données, de la compression des données à la volée, de la déduplication et de la compaction.
- Stockage basé sur la charge de travail, contrôlé par QoS.
- Intégration transparente dans un cloud public pour le Tiering et la protection des données. ONTAP fournit également des fonctionnalités robustes de protection des données qui le distinguent dans tous les environnements :
  - **Copies NetApp Snapshot.** sauvegarde instantanée rapide des données en utilisant un espace disque minimal, sans impact supplémentaire sur les performances.
  - **NetApp SnapMirror.** miroir les copies Snapshot des données d'un système de stockage à un autre. ONTAP prend également en charge la mise en miroir des données vers d'autres plateformes physiques et des services clouds natifs.
  - **SnapLock de NetApp.** pour une administration efficace des données non réinscriptibles, en les écrivant sur des volumes spéciaux qui ne peuvent pas être écrasés ou effacés pour une période déterminée.
  - **NetApp SnapVault.** sauvegarde les données de plusieurs systèmes de stockage sur une copie Snapshot centrale qui sert de sauvegarde à tous les systèmes désignés.
  - **NetApp SyncMirror.** permet la mise en miroir des données en temps réel au niveau RAID sur deux plexes différents de disques connectés physiquement au même contrôleur.
  - **NetApp SnapRestore** permet une restauration rapide des données sauvegardées à la demande à partir de copies Snapshot.
  - **NetApp FlexClone.** assure le provisionnement instantané d'une copie lisible et inscriptible d'un volume NetApp à partir d'une copie Snapshot.

Pour plus d'informations sur ONTAP, consultez le "Centre de documentation ONTAP 9".

NetApp ONTAP est disponible sur site, virtualisé ou dans le cloud.



Plateformes NetApp

NetApp AFF/FAS

NetApp offre des AFF plateformes de stockage FAS (100 % Flash) et scale-out, sur mesure et dotées d'une faible latence, d'une protection des données intégrée et d'une prise en charge multiprotocole.

Ces deux systèmes sont optimisés par le logiciel de gestion des données NetApp ONTAP, le logiciel de gestion des données le plus avancé du secteur pour une gestion du stockage simplifiée, extrêmement disponible et intégrée au cloud qui répond aux besoins de Data Fabric en matière de rapidité, d'efficacité et de sécurité.

Pour en savoir plus sur les plateformes NetApp AFF/FAS, cliquez "ici".

ONTAP Select

ONTAP Select est un déploiement Software-defined de NetApp ONTAP qui peut être déployé sur un hyperviseur de votre environnement. Installée sur VMware vSphere ou KVM, cette solution offre toutes les fonctionnalités et l'expérience d'un système matériel ONTAP.

Pour plus d'informations sur ONTAP Select, cliquez sur "ici".

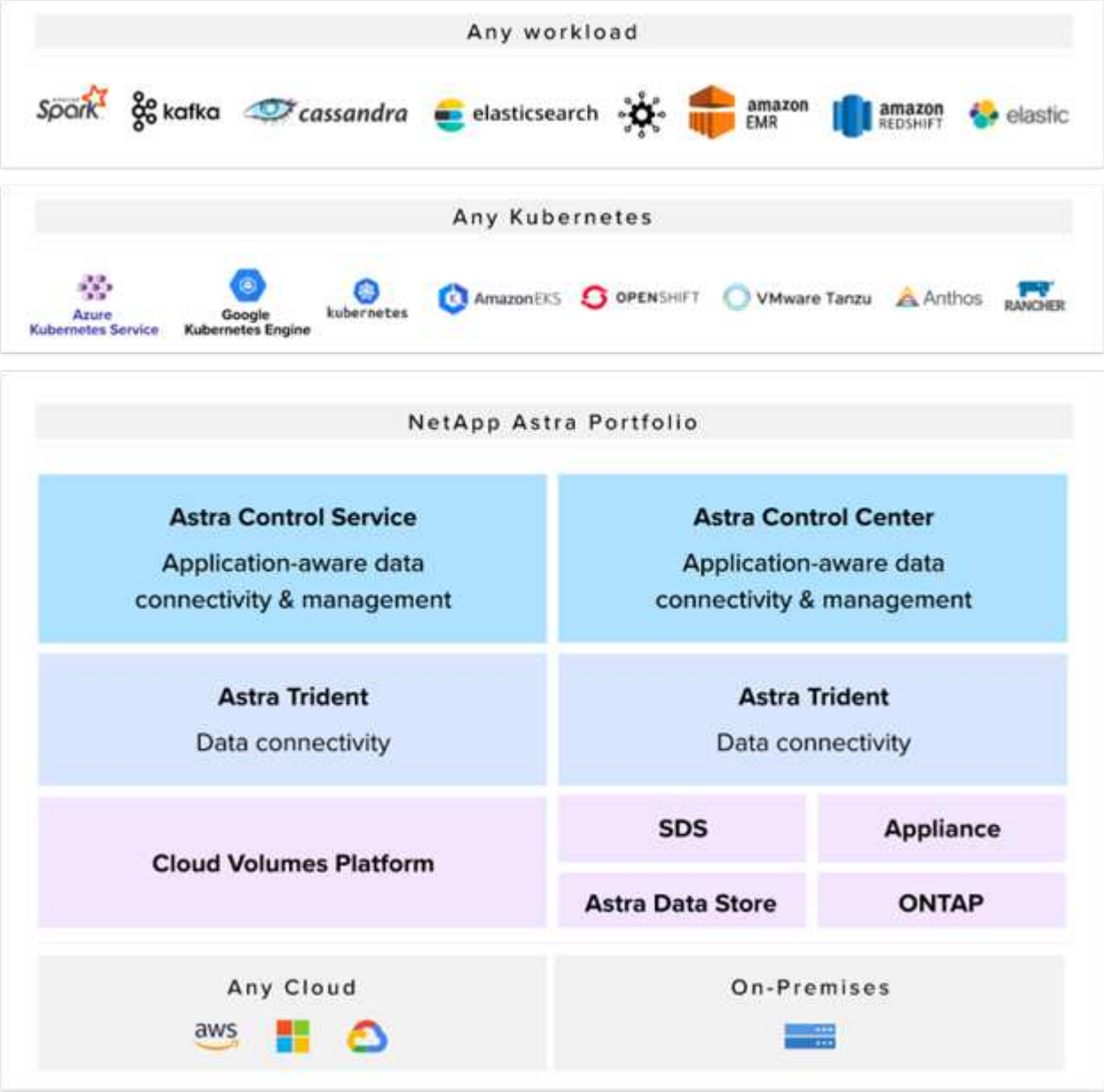
Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP est une version cloud de NetApp ONTAP qui peut être déployée dans un certain nombre de clouds publics, notamment Amazon AWS, Microsoft Azure et Google Cloud.

Pour plus d'informations sur Cloud Volumes ONTAP, cliquez sur "ici".

Présentation de l'intégration du stockage NetApp

NetApp propose plusieurs produits pour orchestrer, gérer, protéger et migrer les applications conteneurisées avec état et leurs données.



NetApp Astra Control propose un ensemble complet de services de gestion du stockage et des données respectueuse des applications pour les workloads Kubernetes avec état optimisés par la technologie de protection des données NetApp. Astra Control Service est disponible pour la prise en charge des workloads avec état dans les déploiements Kubernetes cloud natifs. Le centre de contrôle Astra permet de prendre en charge les workloads avec état dans les déploiements sur site de plateformes Kubernetes d'entreprise telles que Red Hat OpenShift, Rancher, VMware Tanzu etc. Pour en savoir plus, rendez-vous sur le site Web NetApp Astra Control "ici".

NetApp Astra Trident est un orchestrateur de stockage open source entièrement pris en charge pour les conteneurs et les distributions Kubernetes telles que Red Hat OpenShift, Rancher, VMware Tanzu etc. Pour en

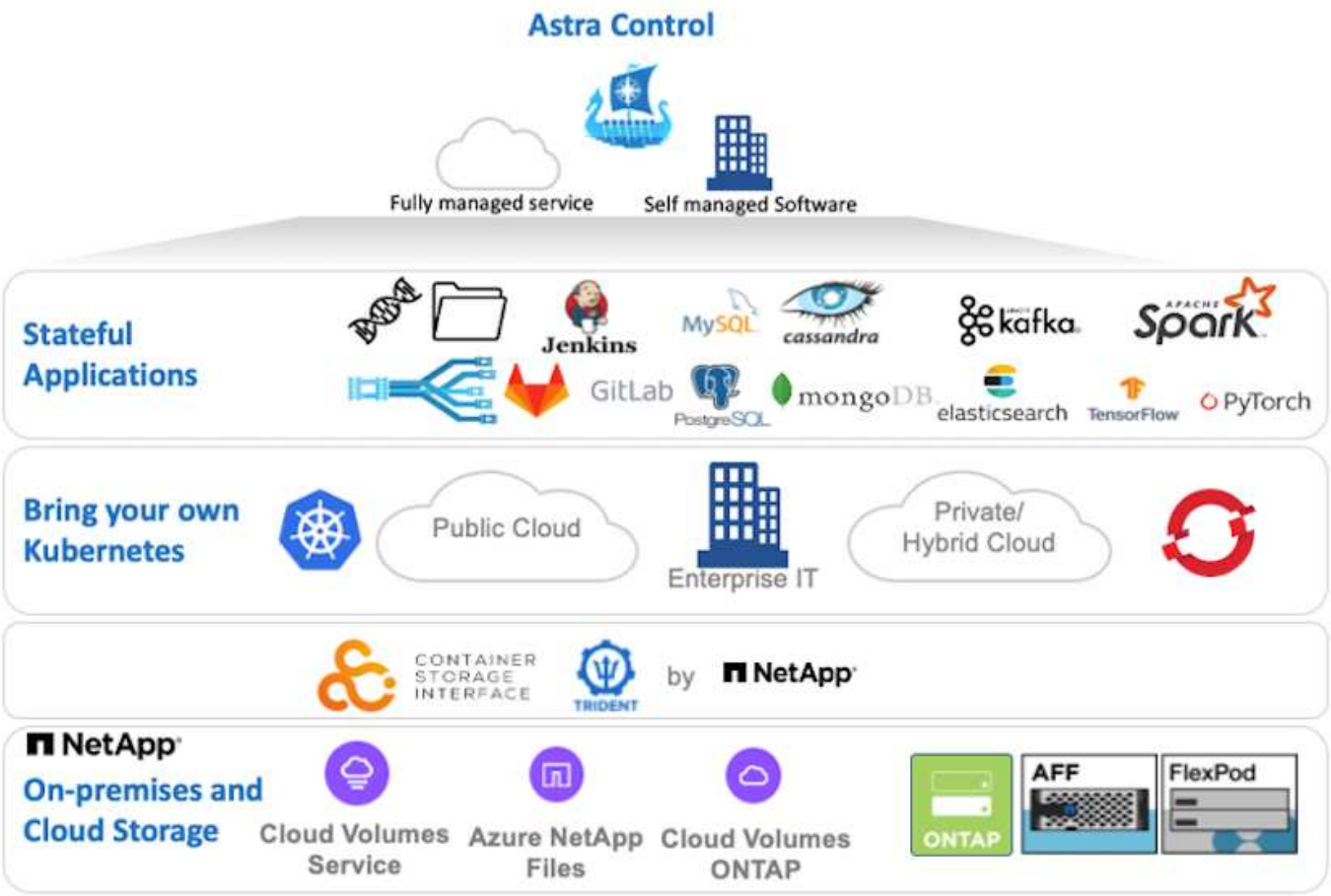
savoir plus, rendez-vous sur le site Web Astra Trident "ici".

Les pages suivantes présentent des informations supplémentaires sur les produits NetApp validés pour les applications et la gestion du stockage persistant dans la solution DevOps with NetApp :

- "NetApp Astra Control Center"
- "NetApp Astra Trident"

Présentation de NetApp Astra Control

NetApp Astra Control Center propose un ensemble complet de services de gestion du stockage et des données respectueuse des applications pour les workloads Kubernetes avec état, déployés dans un environnement sur site et optimisé par les technologies NetApp de protection des données.



Le centre de contrôle NetApp Astra peut être installé sur un cluster Kubernetes sur lequel l'orchestrateur de stockage Astra Trident est déployé et configuré avec des classes de stockage et des systèmes back-end de stockage vers des systèmes de stockage NetApp ONTAP.

Pour en savoir plus sur Astra Trident, rendez-vous sur "ce document ici".

Dans un environnement connecté au cloud, Astra Control Center utilise Cloud Insights pour fournir des fonctionnalités avancées de surveillance et de télémétrie. En l'absence de connexion Cloud Insights, un contrôle limité et une télémétrie (sept jours de metrics) sont disponibles et exportés vers les outils de contrôle natifs Kubernetes (Prometheus et Grafana) via des terminaux ouverts.

Le centre de contrôle Astra est entièrement intégré à l'écosystème NetApp AutoSupport et Active IQ qui fournit

un soutien aux utilisateurs, fournit des conseils pour la résolution de problèmes et affiche des statistiques d'utilisation.

En plus de la version payante d'Astra Control Center, une licence d'évaluation de 90 jours est également disponible. La version d'évaluation est prise en charge par e-mail et dans le Channel Slack de la communauté. Les clients ont accès à ces ressources, à d'autres articles de la base de connaissances et à de la documentation disponibles dans le tableau de bord de support des produits.

Pour en savoir plus sur la gamme Astra, consultez le "Site Web d'Astra".

Pour obtenir un guide d'installation et d'exploitation détaillé sur le centre de contrôle Astra, suivez la documentation "ici".

Automatisation du centre de contrôle Astra

Astra Control Center est doté d'une API REST entièrement fonctionnelle pour l'accès par programmation. Les utilisateurs peuvent utiliser n'importe quel langage ou utilitaire de programmation pour interagir avec les terminaux API REST Astra Control. Pour plus d'informations sur cette API, reportez-vous à la documentation "ici".

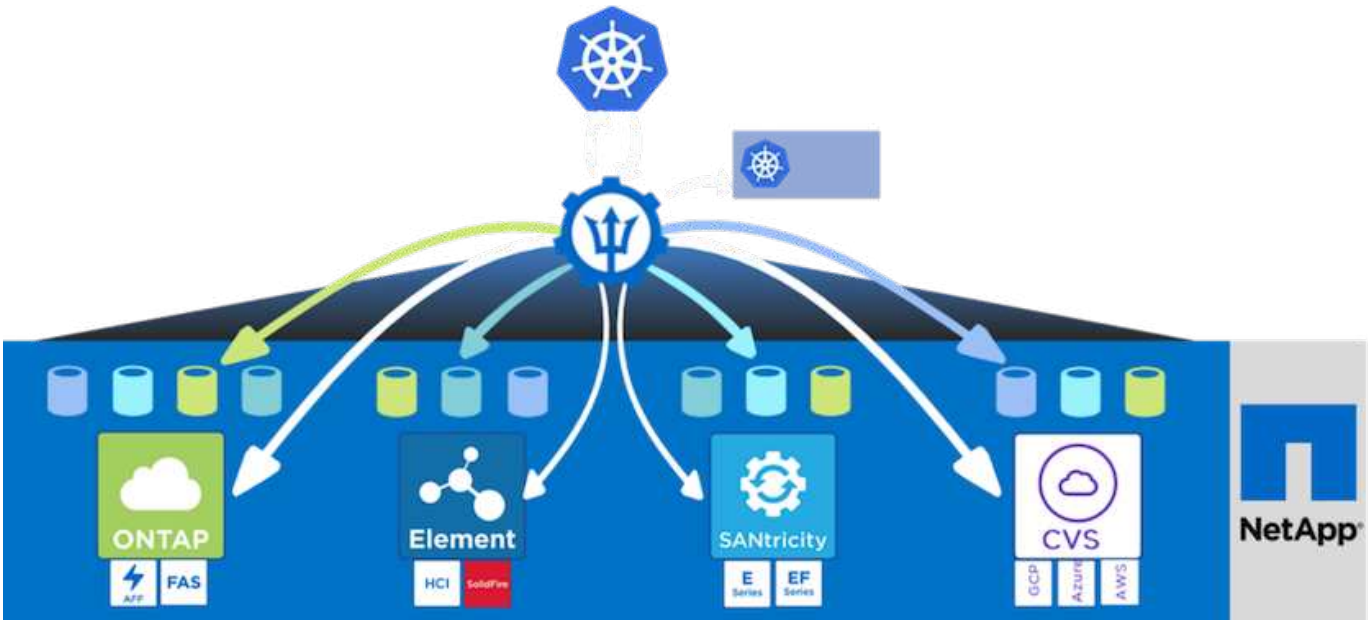
Si vous recherchez un kit de développement logiciel prêt à l'emploi pour interagir avec les API REST Astra Control, NetApp propose un kit avec le kit SDK Python Astra Control que vous pouvez télécharger "ici".

Si la programmation n'est pas propriétaire de votre situation et si vous souhaitez utiliser un outil de gestion de la configuration, vous pouvez cloner et exécuter les playbooks Ansible publiés par NetApp "ici".

Présentation d'Astra Trident

Astra Trident est un orchestrateur de stockage open source entièrement pris en charge pour les conteneurs et les distributions Kubernetes telles que Red Hat OpenShift, VMware Tanzu, Anthos by Google Cloud, Rancher etc. Trident fonctionne avec l'ensemble de la gamme de solutions de stockage NetApp, notamment les systèmes de stockage NetApp ONTAP et Element, et prend également en charge les connexions NFS et iSCSI. Trident accélère le workflow DevOps en permettant aux utilisateurs d'approvisionner et de gérer le stockage à partir de leurs systèmes de stockage NetApp, sans intervention de l'administrateur de stockage.

Un administrateur peut configurer plusieurs systèmes de stockage back-end en fonction des besoins des projets et des modèles de système de stockage. Ces fonctionnalités permettent notamment la compression, des types de disques spécifiques ou des niveaux de QoS garantissant un certain niveau de performance. Une fois définis, ces systèmes back-end peuvent être utilisés par les développeurs dans leurs projets pour créer des demandes de volume persistant et connecter le stockage persistant à la demande dans leurs conteneurs.



Astra Trident a un cycle de développement rapide et, comme Kubernetes, est lancé quatre fois par an.

La dernière version d'Astra Trident est disponible en avril 22.04, en avril 2022. Une matrice de prise en charge pour quelle version de Trident a été testée avec laquelle une distribution Kubernetes est disponible "ici".

Depuis la version 20.04, l'opérateur Trident effectue la configuration de Trident. L'opérateur facilite les déploiements à grande échelle et offre un support supplémentaire, notamment l'auto-rétablissement des pods déployés dans le cadre de l'installation de Trident.

Avec la version 21.01, un graphique Helm a été disponible pour faciliter l'installation de l'opérateur Trident.

Reportez-vous à la documentation "ici" Pour installer et utiliser Astra Trident.

Validation du cas d'utilisation : le DevOps avec NetApp Astra

Les utilisations suivantes ont été validées avec NetApp Astra, pour le DevOps :

- "Protection intégrée avec les pipelines ci/CD et NetApp Astra Control"
- "Contrôlez Astra pour faciliter l'analyse post-mortem et la restauration de l'application"
- "Accélération du développement logiciel avec NetApp FlexClones"

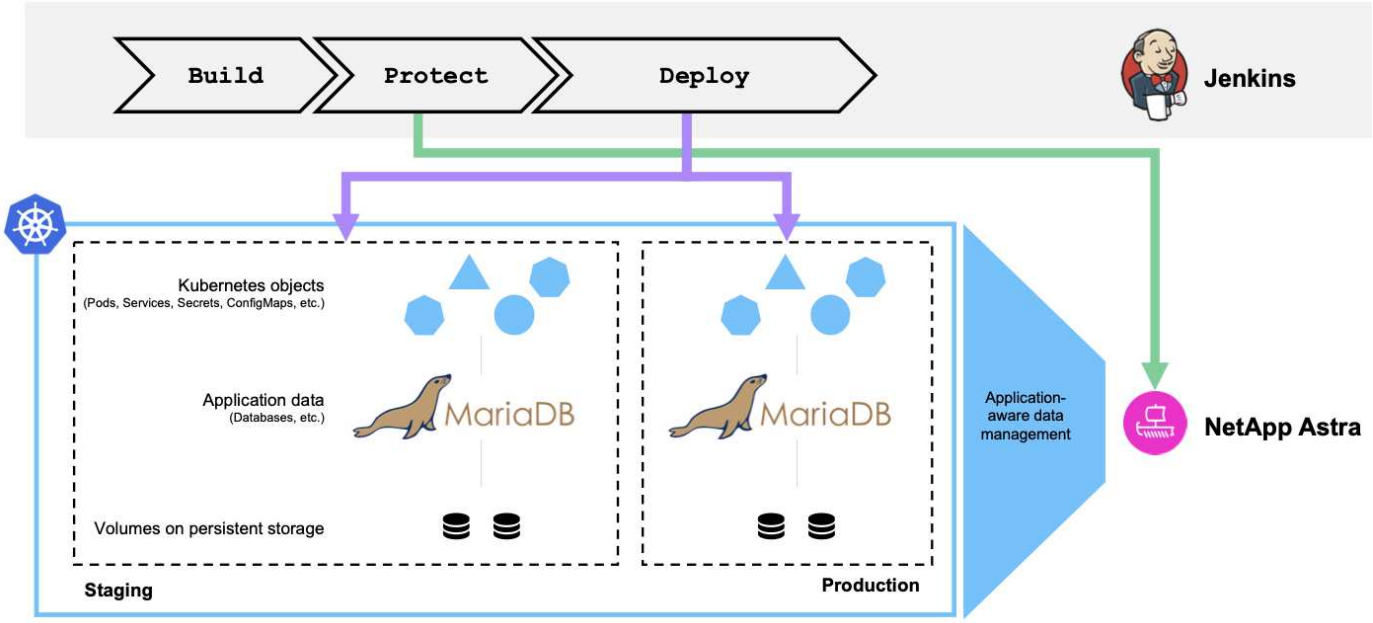
Protection intégrée avec les pipelines ci/CD et NetApp Astra Control

Présentation

L'une des utilisations les plus courantes des workflows DevOps est l'intégration continue et les pipelines de déploiement continu qui créent, intègrent et exécutent des suites de tests automatisés sur des applications lors de l'exécution du nouveau code par les développeurs. Les ingénieurs DevOps et les ingénieurs de fiabilité des sites (SRE) ont généralement mis en œuvre des pipelines dédiés au développement de nouvelles fonctionnalités, aux tests de régression, aux correctifs, à l'ingénierie de la qualité et à d'autres fonctions dans le processus de développement.

À mesure que les équipes augmentent leur niveau d'automatisation, le rythme des changements dans les applications de production peut sembler compliqué. Par conséquent, certaines équipes préfèrent protéger les applications ou les services de production. Outre la protection des images du code et du conteneur, ils souhaitent également protéger l'état de l'application, les données de configuration (objets Kubernetes et ressources associées à l'application, par exemple) et les données persistantes d'une application.

Dans ce cas d'utilisation, nous examinons de plus près un pipeline de promotion en production qui déploie une nouvelle version d'une application : d'abord dans un environnement intermédiaire, puis dans un environnement de production. Cet exemple s'applique aussi bien aux principaux clouds publics que à un environnement sur site. Bien que nous montrons le déploiement d'une version de l'app, le pipeline peut également être utilisé avec d'autres stratégies, telles que le déploiement bleu/vert ou canari. Dans le cadre du pipeline ci/CD, nous allons protéger l'application en créant une sauvegarde complète de l'application. De nombreux workflows DevOps peuvent être utiles pour une sauvegarde de l'application en production intégrant la cohérence applicative, ainsi que ses données, son état et sa configuration.



L'application utilisée pour valider ce cas d'utilisation était "Magento", Une solution de commerce électronique avec un front-end basé sur le Web, une instance Elasticsearch pour des fonctions de recherche et d'analyse et une base de données MariaDB qui suit tous les détails de l'inventaire des achats et des transactions. Cette application conteneurisée a été installée sur un cluster Red Hat OpenShift. Chaque pod de l'application utilisait des volumes persistants pour stocker les données. Les volumes persistants ont été automatiquement créés par NetApp Astra Trident, l'orchestrateur de stockage conforme à l'interface de conteneur pour Kubernetes, qui permet de provisionner le stockage sur des systèmes de stockage NetApp. En outre, avec les fonctionnalités de protection des applications d'Astra Control Center, l'application en question a été gérée par Astra Control, qui a ensuite été utilisée pour déclencher les sauvegardes d'application qui stockaient l'état de l'application ainsi que les données stockées dans des volumes persistants. Nous avons utilisé "Kit de développement logiciel NetApp Astra Control Python" Automatiser le processus de déclenchement des sauvegardes d'applications ; celles-ci ont ensuite été intégrées ou CD dans un pipeline. Ce pipeline a été créé et exécuté à l'aide d'un outil ci/CD appelé ["Jenkins"] automatiser le flux pour créer, protéger et déployer l'application.

Passons en revue les conditions préalables et la procédure pour introduire la protection dans un pipeline ci/CD.

Conditions préalables à la validation du cas d'utilisation

Les outils ou plates-formes suivants ont été déployés et configurés comme conditions préalables :

1. Plateforme de conteneurs Red Hat OpenShift
2. NetApp Astra Trident a été installé sur OpenShift avec un système back-end configuré pour le système NetApp ONTAP
3. Configuration par défaut de storageclass pointant sur un back-end NetApp ONTAP
4. NetApp Astra Control Center installé sur un cluster OpenShift
5. Cluster OpenShift ajouté en tant que cluster géré à Astra Control Center
6. Jenkins a installé sur un cluster OpenShift et configuré avec un nœud agent sur lequel un moteur Docker est installé

Installation de l'application

Commençons par l'installation initiale de l'application dans les environnements de stockage et de production. Pour les besoins de ce cas d'utilisation, cette étape est un prérequis, cette opération est effectuée manuellement. Le pipeline ci/CD est utilisé pour les workflows de création et de déploiement ultérieurs suite à la sortie de nouvelle version de l'application.

Dans ce cas d'utilisation, l'environnement de production est un espace de nom appelé `magento-prod`, et l'environnement de staging correspondant est un espace de noms appelé `magento-staging` Configuré sur le cluster Red Hat OpenShift. Pour passer à l'application, procédez comme suit :

1. Installez l'application Magento à l'aide du graphique de bitnami Helm sur l'environnement de production. Nous utilisons RWX PVS pour les pods Magento et 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
   ```

   > Le diagramme de gouvernail Magento bitnami nécessite un service LoadBalancer pour exposer le service GUI de Magento. Nous avons utilisé "MetalLB" dans cet exemple, vous pouvez fournir un service d'équilibrage de charge sur site.

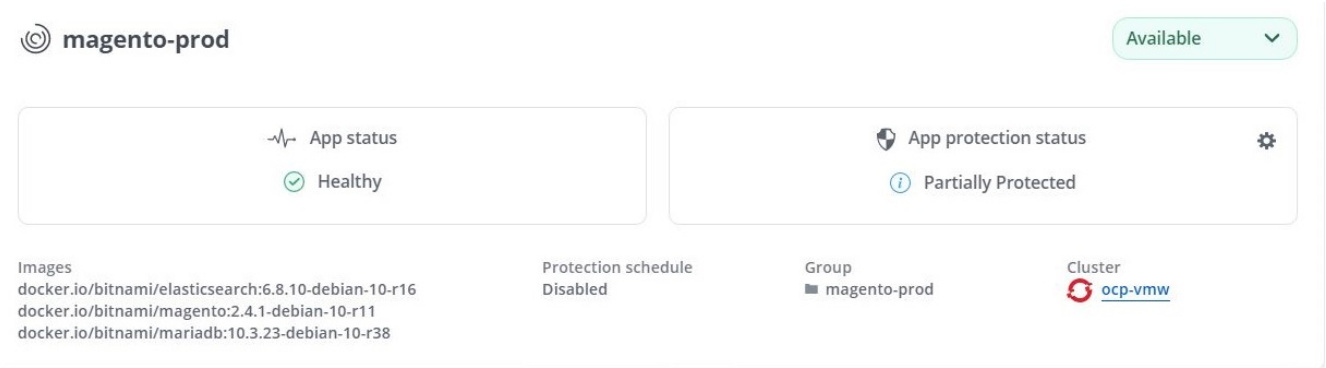
2. Après quelques minutes, vérifiez que tous les pods et services sont en cours d'exécution.

```
[netapp-user@rhel7 na_astra_control_suite]$ oc get pods -n magento-prod
NAME                                                    READY   STATUS
RESTARTS   AGE
magento-9d658fd96-qrxmt                                 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. Répétez la même procédure pour l'environnement de staging.

Gérer l'application Magento dans Astra Control Center

1. Accédez à applications et sélectionnez l'onglet applications découvertes.
2. Cliquez sur les points de suspension par rapport à l'application Magento dans l'environnement de production (`magento-prod`), puis cliquez sur gérer.
3. L'application Magento est désormais gérée par Astra Control Center. Toutes les opérations prises en charge par Astra Control peuvent être exécutées sur l'application. Notez également la version de l'application.



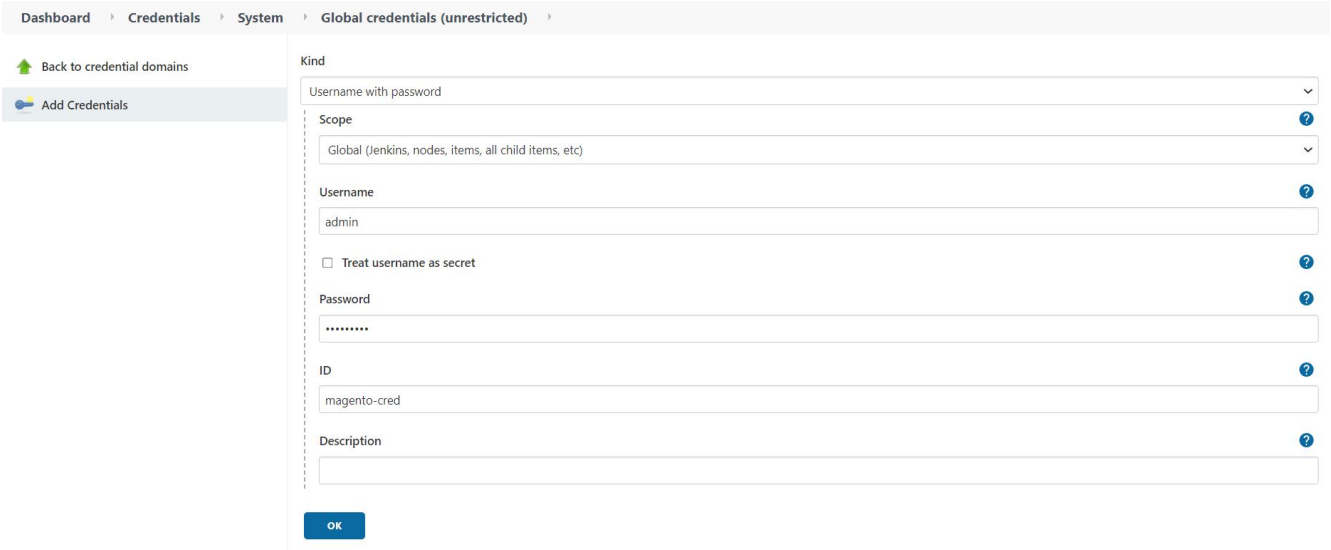
4. Répétez les étapes de gestion de l'application Magento dans l'environnement de staging (`magento-staging`).

Pipeline ci/CD avec protection intégrée

Lorsque nous utilisons de nouvelles versions d'applications, nous utilisons un pipeline ci/CD pour créer l'image de conteneur, sauvegarder les environnements de stockage intermédiaire et de production, déployer la nouvelle version de l'application dans l'environnement intermédiaire, attendre l'approbation pour la promotion de la production, puis déployez la nouvelle version de l'application dans l'environnement de production. Pour utiliser un pipeline ci/CD, procédez comme suit :

1. Connectez-vous à Jenkins et créez les informations d'identification requises : un pour les crds Magento, un pour les crds d'administration MariaDB, et le troisième pour les crds racine MariaDB.

2. Accédez à Manage Jenkins > Manage Credentials et cliquez sur le domaine approprié.
3. Cliquez sur Ajouter des informations d'identification et définissez le type sur Nom d'utilisateur avec le mot de passe et la portée définis sur Global. Entrez le nom d'utilisateur, le mot de passe et un ID pour les informations d'identification, puis cliquez sur OK.

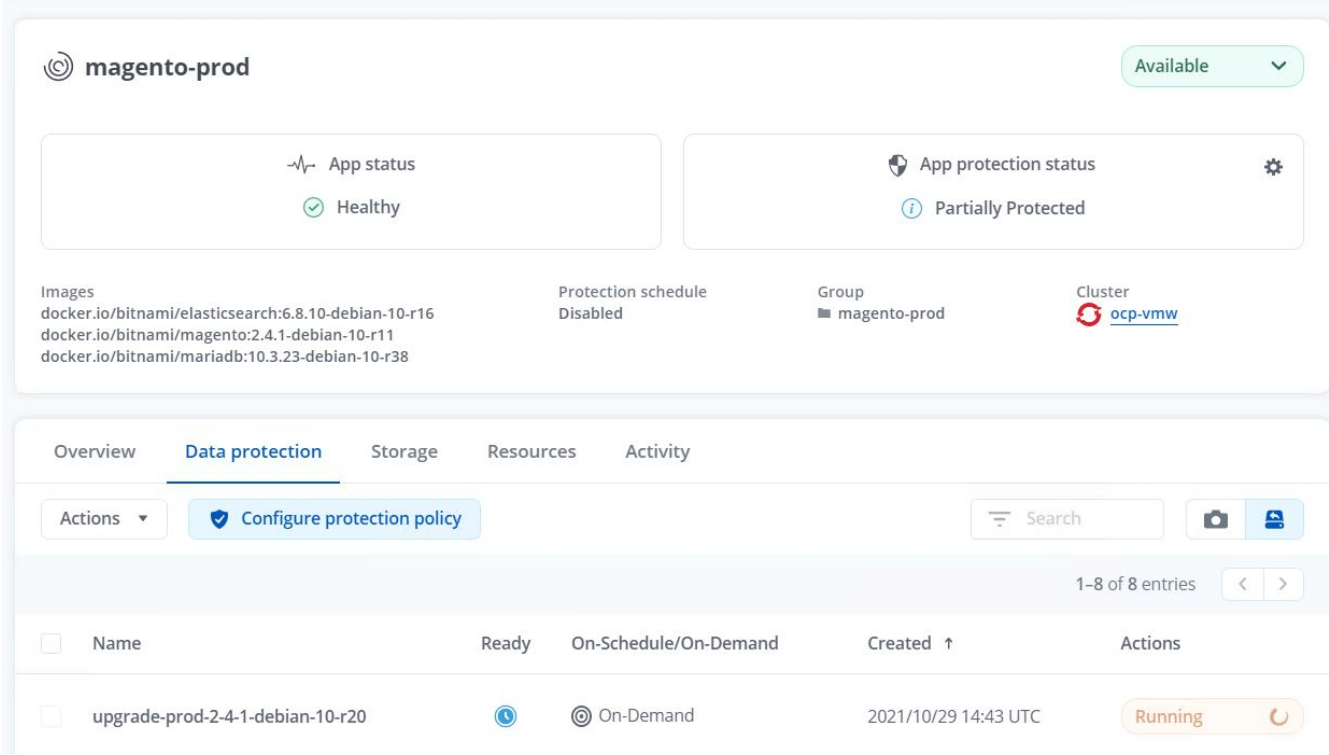


4. Répétez la même procédure pour les deux autres identifiants.
5. Retournez au tableau de bord, créez un pipeline en cliquant sur nouvel élément, puis cliquez sur Pipeline.
6. Copiez le pipeline à partir du fichier Jenkinsfile "ici".
7. Collez le pipeline dans la section Jenkins Pipeline, puis cliquez sur Save.
8. Remplissez les paramètres du pipeline Jenkins avec les détails respectifs, y compris la version du graphique Helm, la version de l'application Magento à mettre à niveau, la version de la boîte à outils Astra, le FQDN Astra Control Center, le jeton API et son ID d'instance. Spécifiez le registre docker, l'espace de noms et l'adresse IP Magento des environnements de production et de staging, ainsi que les ID d'identification des informations d'identification créées.

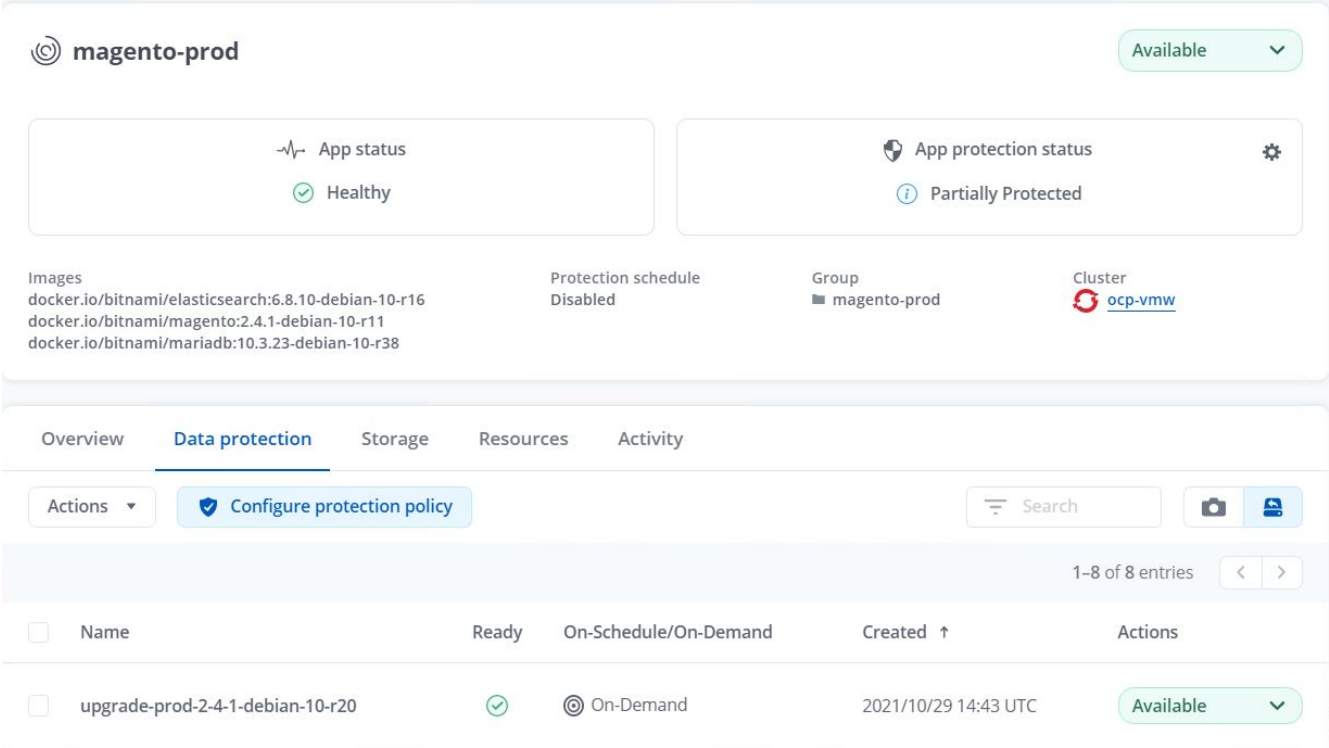
```
MAGENTO_VERSION = '2.4.1-debian-10-r14'
CHART_VERSION = '14'
RELEASE_TYPE = 'MINOR'
ASTRA_TOOLKIT_VERSION = '2.0.2'
ASTRA_API_TOKEN = 'xxxxxxxx'
ASTRA_INSTANCE_ID = 'xxx-xxx-xxx-xxx-xxx'
ASTRA_FQDN = 'netapp-astra-control-center.org.example.com'
DOCKER_REGISTRY = 'docker.io/netapp-solutions-cicd'
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. Cliquez sur Créer maintenant. Le pipeline commence à exécuter et progresse à travers les étapes. L'image de l'application est d'abord créée et téléchargée dans le registre du conteneur.

10. Les sauvegardes d'applications sont lancées par Astra Control.

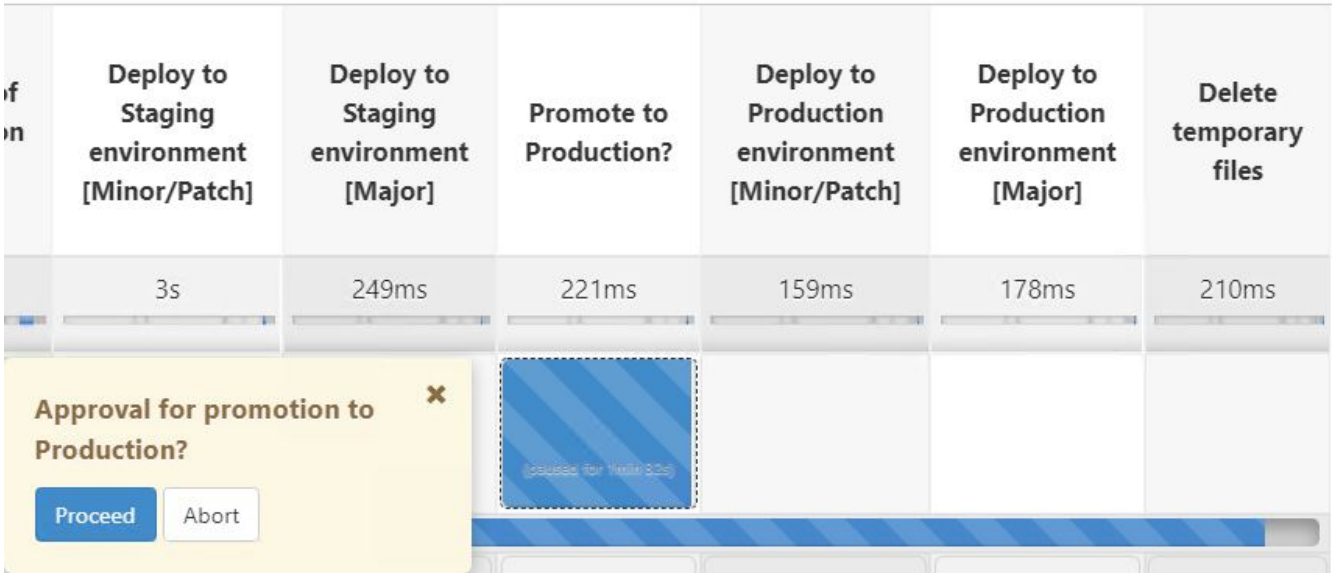


11. Une fois les étapes de sauvegarde terminées, vérifiez les sauvegardes à partir du centre de contrôle Astra.

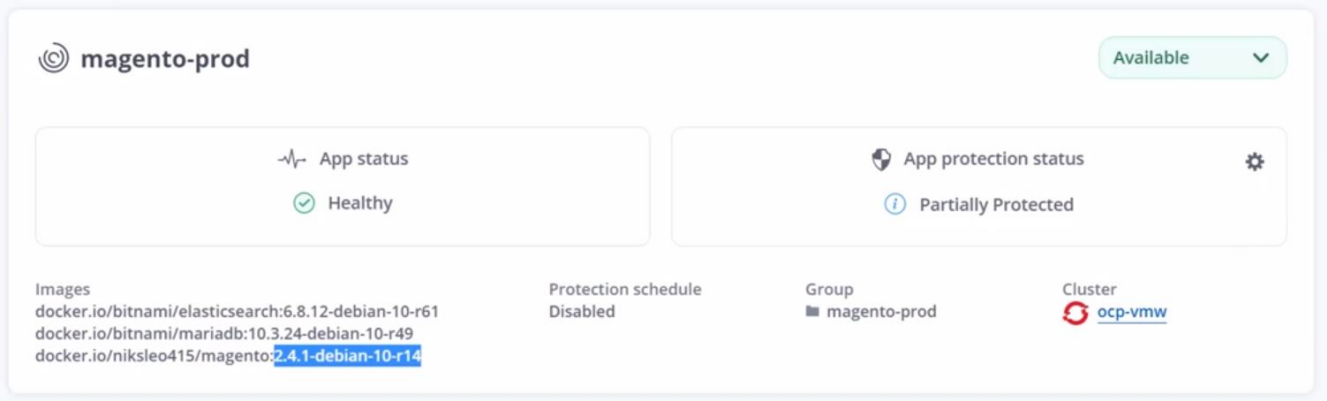


12. La nouvelle version de l’application est ensuite déployée dans l’environnement temporaire.

13. Une fois cette étape terminée, le programme attend que l’utilisateur approuve le déploiement en production. À ce stade, supposons que l’équipe QA effectue des tests manuels et approuve la production. Vous pouvez ensuite cliquer sur approuver pour déployer la nouvelle version de l’application dans l’environnement de production.



14. Vérifiez que l'application de production est également mise à niveau vers la version souhaitée.



Dans le cadre du pipeline ci/CD, nous avons démontré la capacité à protéger l'application par la création d'une sauvegarde complète intégrant la cohérence applicative. Dans la mesure où l'application complète a été sauvegardée dans le cadre du pipeline de promotion à production, vous êtes davantage confiant en matière de déploiements d'applications hautement automatisés. Cette sauvegarde respectueuse des applications, incluant les données, l'état et la configuration de l'application, peut s'avérer utile pour de nombreux workflows DevOps. Un workflow important serait de revenir à la version précédente de l'application en cas de problèmes imprévus.

Bien que nous ayons démontré un workflow ci/CD avec l'outil Jenkins, le concept peut être extrapolé facilement et efficacement à différents outils et stratégies. Pour voir ce cas d'utilisation en action, regardez la vidéo "ici".

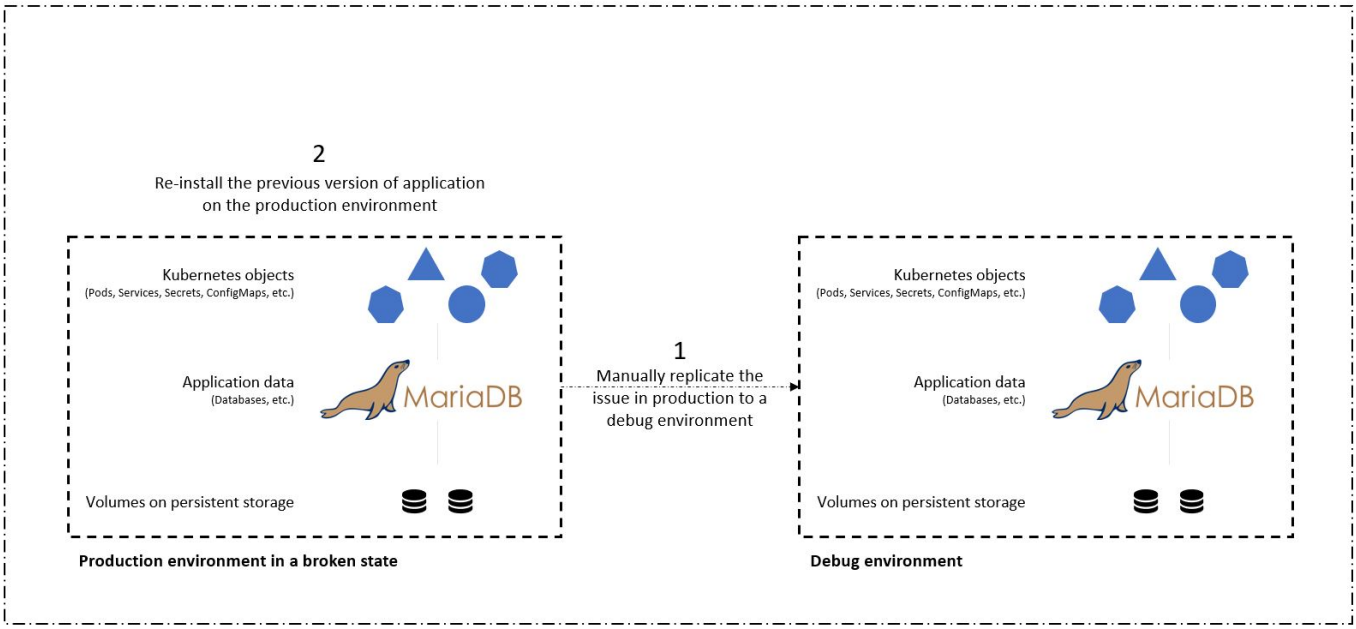
Utilisez Astra Control pour faciliter l'analyse post-mortem et restaurer l'application

Présentation

Dans le "première utilisation", Nous avons démontré comment utiliser NetApp Astra Control Center pour protéger vos applications dans Kubernetes. Cette section décrit comment intégrer les sauvegardes d'applications via Astra Control directement dans votre workflow de développement à l'aide du kit de développement Python du kit NetApp Astra. Cette approche permet de protéger les environnements de

développement et de production en automatisant les sauvegardes à la demande lors du processus d'intégration et de déploiement continus (ci/CD). Avec cette couche supplémentaire de protection des données cohérente au niveau des applications ajoutée au pipeline ci/CD et aux applications de production, les processus de développement sont en sécurité en cas de problème, ce qui favorise la continuité de l'activité.

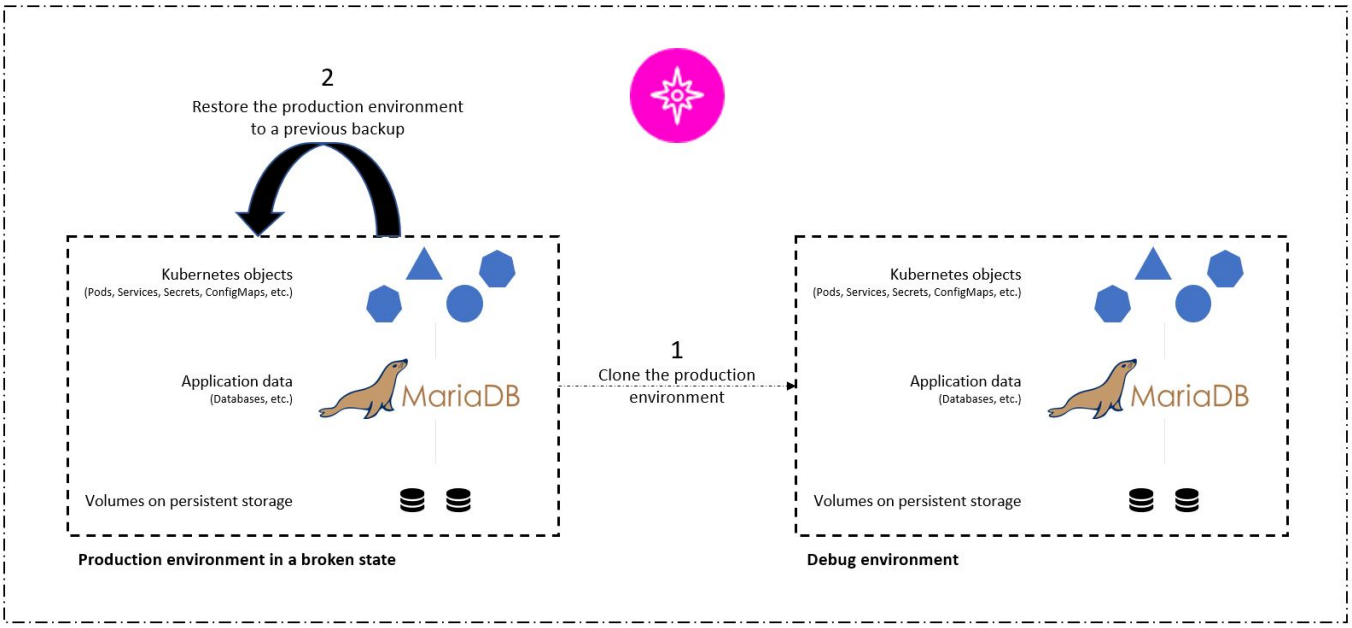
Dans un workflow classique, après avoir rencontré un échec lors de la mise à niveau de l'application vers une nouvelle version, l'équipe de développement tenterait de résoudre le problème en temps réel en fonction des rapports de bogues fournis par les clients. Au premier signe de problème, l'équipe pourrait également tenter de redéployer l'application vers un environnement de débogage parallèle pour mettre ce processus hors ligne. Ils pouvaient redéployer une ancienne base de codes depuis une version précédente vers la production, afin de restaurer l'application en bon état de fonctionnement.



Bien que cette approche fonctionne, l'équipe doit s'assurer que l'état de l'application de production défaillante correspond à celui de la version utilisée en production lorsque le problème survient. Il leur faudrait également consacrer du temps à promouvoir la version fiable en production en récupérant du code de leur référentiel et en redéployant les images de la machine pour restaurer l'application à un état de fonctionnement correct. De plus, dans ce scénario, nous ne voulions pas si la base de données de production elle-même était corrompue par le code défectueux. Idéalement, il existe des processus de sauvegarde distincts pour les données de la base de données, mais devons-nous supposer qu'ils sont cohérents avec l'état de l'application tel qu'il a été publié ? C'est là que les avantages offerts par Astra Control, notamment en matière de sauvegardes, de restaurations et de clones avec état et cohérents au niveau des applications, montrent véritablement leur valeur.

Nous pouvons tout d'abord utiliser Astra Control pour faciliter l'analyse post-mortem de l'état de l'application. Pour ce faire, nous clonons la version de production buggy vers un environnement de test parallèle de façon cohérente avec l'application. Cet environnement étant mis de côté, nous pouvons résoudre le problème en temps réel.

De plus, Astra Control prend en charge la fonctionnalité de restauration sur place qui nous permet de restaurer l'application de production vers une dernière sauvegarde acceptable (qui a précédé la version de code affligée). La version restaurée suppose la position de l'application de production buggy précédente, de façon cohérente avec les applications et avec état, y compris l'IP d'entrée précédemment attribuée. Par conséquent, les clients qui accèdent à l'environnement frontal ne connaissent pas la transition vers la version de sauvegarde.



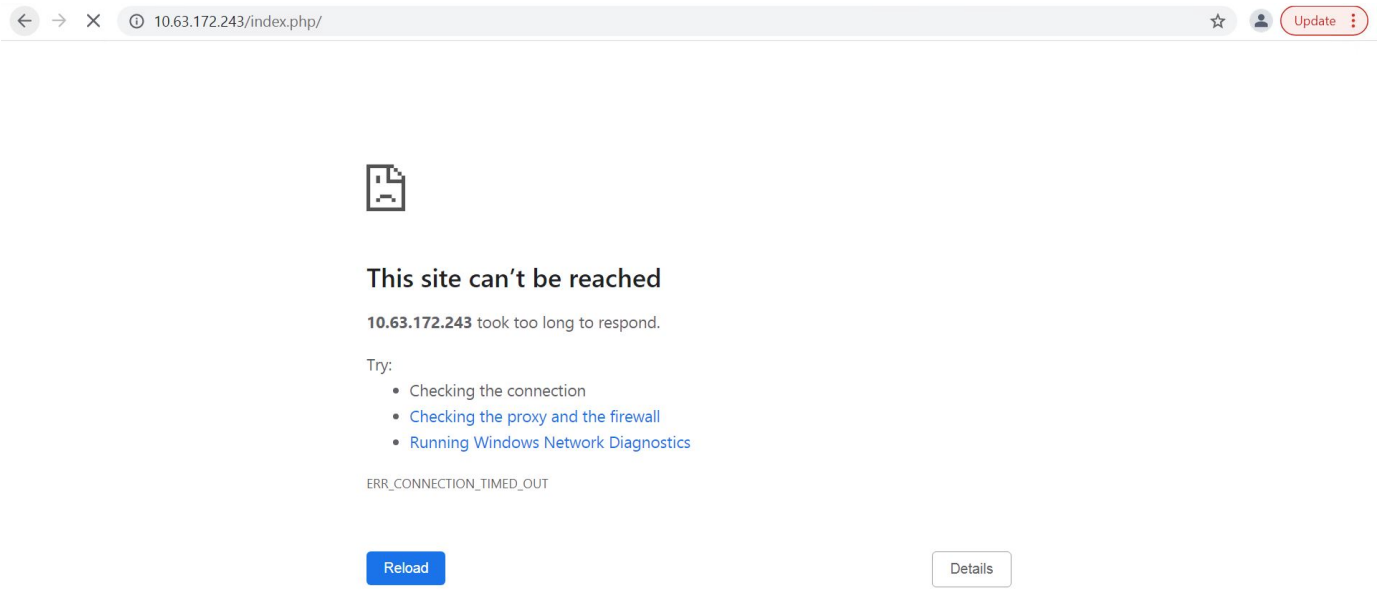
Conditions préalables à la validation du cas d'utilisation

Les outils ou plates-formes suivants ont été déployés et configurés comme conditions préalables :

- Plateforme de conteneurs Red Hat OpenShift.
- NetApp Astra Trident installé sur OpenShift avec un système back-end configuré sur un système NetApp ONTAP.
- Configuration par défaut de storageclass pointant sur un back-end NetApp ONTAP.
- NetApp Astra Control Center installé sur un cluster OpenShift.
- Cluster OpenShift ajouté en tant que cluster géré à Astra Control Center.
- Jenkins installé sur un cluster OpenShift.
- Application Magento installée dans l'environnement de production. Dans ce cas d'utilisation, l'environnement de production est un espace de nom appelé « agento-prod » dans un cluster Red Hat OpenShift.
- Application de production gérée par Astra Control Center.
- Sauvegarde(s) fiable(s) de l'application de production capturée avec Astra Control.

Cloner et restaurer le pipeline

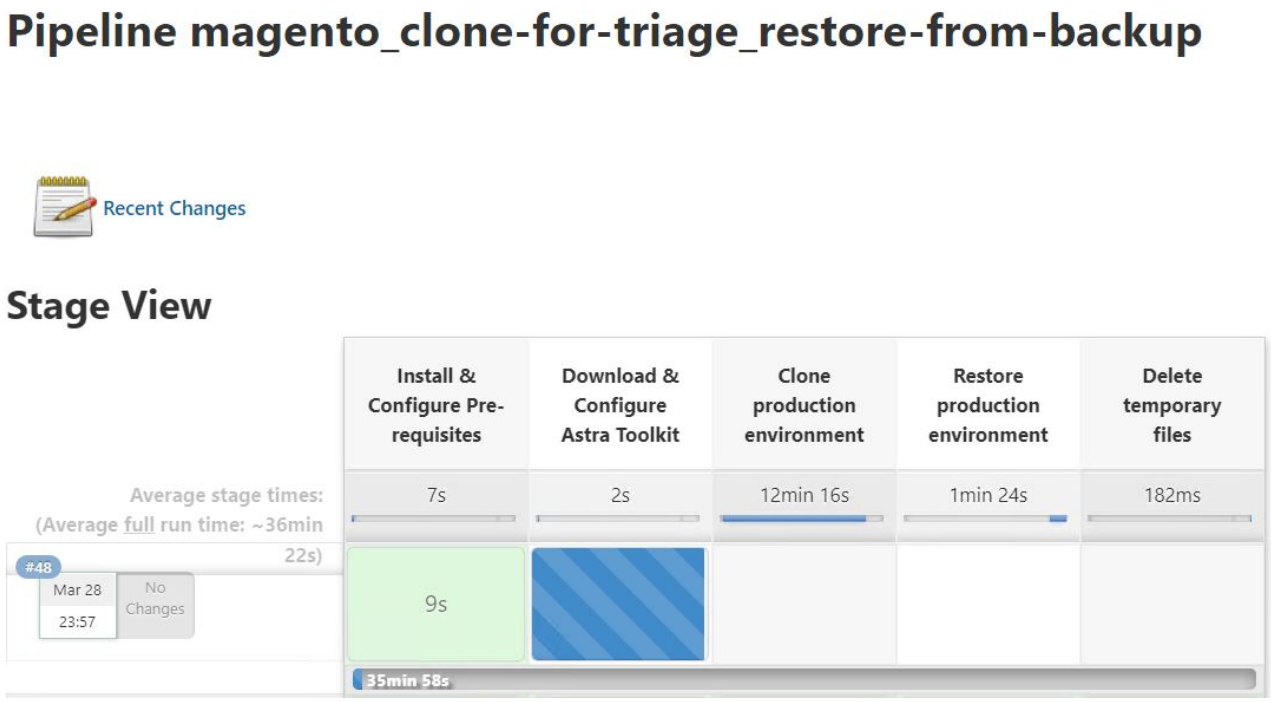
Compte tenu du fait que l'application a été mise à niveau vers une nouvelle version, l'application dans l'environnement de production (`magento-prod`) ne se comporte pas comme prévu après la mise à niveau. Supposons que les données renvoyées par les requêtes frontales ne correspondent pas à la demande ou que la base de données a été endommagée. Pour cloner et restaurer le pipeline, effectuez la procédure suivante :



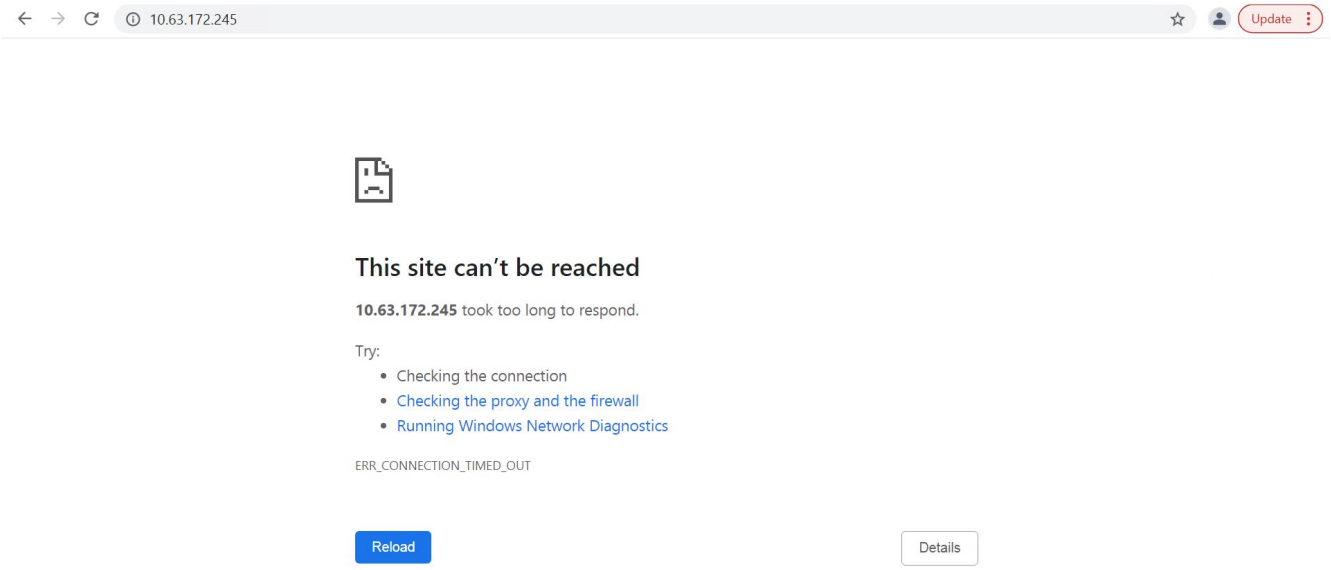
1. Connectez-vous à Jenkins et créez un pipeline en cliquant sur nouvel élément, puis sur Pipeline.
2. Copiez le pipeline à partir du fichier Jenkinsfile "ici".
3. Collez le pipeline dans la section Jenkins Pipeline, puis cliquez sur Save.
4. Remplissez les paramètres du pipeline Jenkins avec les détails respectifs tels que la version actuelle de l'application Magento en production, le FQDN Astra Control Center, le jeton API, l'ID d'instance et le nom d'application ou l'espace de noms d'environnements de production et de débogage, ainsi que les noms de cluster source et de destination. Dans le cadre de cette utilisation, l'environnement de production est un espace de noms appelé « agento-prod » et l'environnement de débogage est un espace de noms appelé « agento-debug » configuré sur un cluster Red Hat OpenShift.

```
MAGENTO_VERSION = '2.4.1-debian-10-r14'
ASTRA_TOOLKIT_VERSION = '2.0.2'
ASTRA_API_TOKEN = 'xxxxx'
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'
```

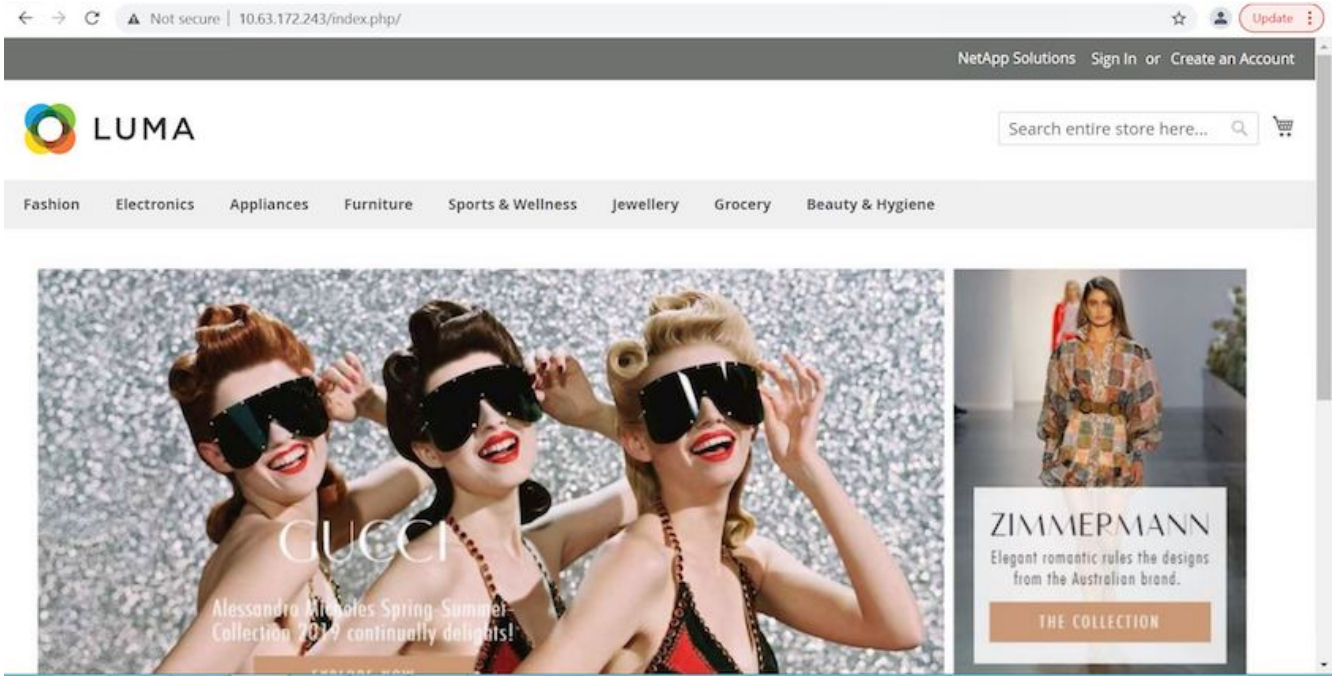
5. Cliquez sur Créer maintenant. Le pipeline commence à exécuter et progresse à travers les étapes. L'application est d'abord clonée dans l'état actuel dans un environnement de débogage, et l'application est ensuite restaurée dans la sauvegarde dont le fonctionnement a été vérifié.



6. Vérifiez que l’application clonée est la version contenant le bogue.



7. Vérifiez que l’environnement de production est restauré sur une sauvegarde de travail et que l’application en production fonctionne comme prévu.



Ces deux opérations en tandem accélèrent le retour au fonctionnement normal de l'entreprise. Pour voir ce cas d'utilisation en action, regardez la vidéo "ici".

Accélération du développement logiciel avec la technologie NetApp FlexClone

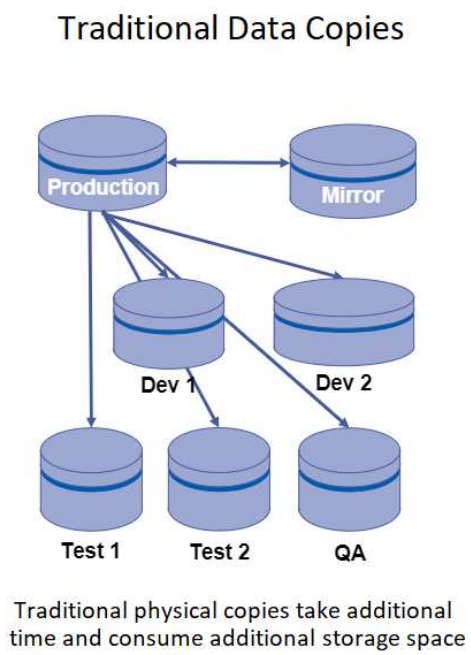
Présentation

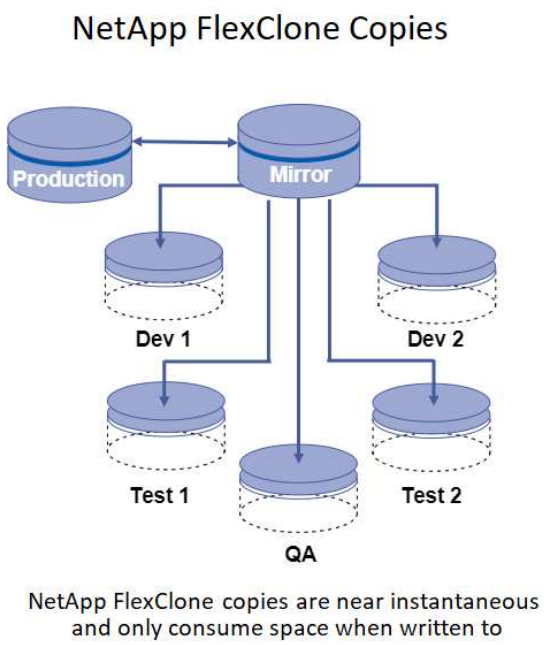
Le clonage d'une application déployée dans un cluster Kubernetes est un outil très utile pour les développeurs qui souhaitent accélérer leurs workflows en partageant des environnements avec des partenaires ou en testant de nouvelles versions de code dans un environnement de développement sans interférer avec la version sur laquelle ils travaillent actuellement. Le clonage avec état et cohérence applicative d'une application Kubernetes est une fonctionnalité majeure incluse avec NetApp Astra Control, ainsi que la sauvegarde et la restauration des applications. Par ailleurs, si une application est clonée dans le même cluster Kubernetes avec le même système back-end de stockage, Astra Control utilise par défaut la technologie NetApp FlexClone pour la duplication des volumes de données persistants, accélérant ainsi le processus de façon significative. En accélérant ce processus, l'environnement cloné est provisionné et peut être utilisé en quelques instants. Les développeurs peuvent ainsi reprendre leur travail avec une courte pause lorsque l'on compare le redéploiement de leur environnement de test et de développement. Pour plus de commodité, vous pouvez appeler toutes les fonctions de NetApp Astra Control avec une API, qui facilite l'intégration dans les frameworks d'automatisation comme Ansible. Ainsi, les environnements peuvent être échelonnés encore plus rapidement, car seules des modifications mineures sont nécessaires dans un manuel de vente ou un rôle pour lancer la procédure de clonage.

Qu'est-ce que la technologie NetApp FlexClone ?

La technologie NetApp FlexClone est une copie Snapshot inscriptible instantanée à partir d'un environnement NetApp FlexVol. Elles sont provisionnées presque instantanément, contiennent toutes les données du volume source et ne consomment aucun espace de stockage supplémentaire tant que les données du nouveau volume ne sont pas nouvelles de la source. Elles sont souvent utilisées dans des environnements de développement ou basés sur des modèles lorsque plusieurs copies de données sont utiles pour la mise en scène ; les systèmes de stockage disposent de ressources limitées pour le provisionnement de ces volumes. Par rapport à un système de stockage traditionnel dans lequel les données doivent être copiées plusieurs fois plus vite et consommation d'espace de stockage important, la technologie NetApp FlexClone accélère les

tâches dépendantes du stockage.





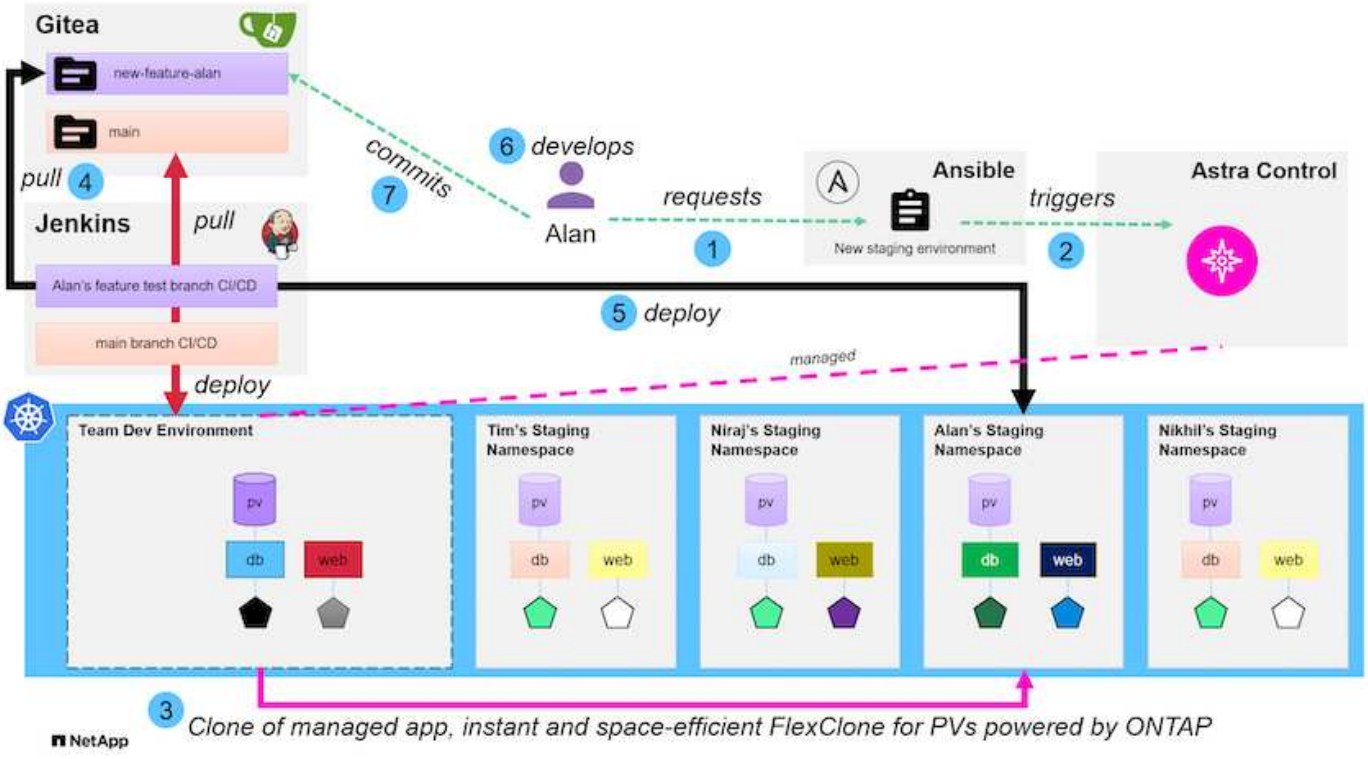
Pour en savoir plus sur la technologie NetApp FlexClone, consultez la page "Documents NetApp".

Prérequis

1. Une distribution Kubernetes prise en charge, telle que Red Hat OpenShift 4.6.8+, Rancher 2.5+ ou Kubernetes 1.19+.
2. NetApp Astra Control Center, 21.12+.
3. Un système NetApp ONTAP avec un système back-end de stockage configuré via NetApp Astra Trident.
4. Ansible 2.9+.
5. Des modèles pour les environnements que vous souhaitez cloner en tant qu'applications gérées dans NetApp Astra Control.

Introduction au cas d'utilisation

Pour cette utilisation, nous visualisons un environnement similaire à celui-ci :



1. Un utilisateur exécute ce manuel de vente ansible pour créer un nouvel environnement intermédiaire.
2. Ansible utilise le module URI-API pour appeler Astra Control afin d'exécuter l'opération de clonage.
3. Astra Control exécute une opération de clonage sur un environnement modèle préprovisionné, créant ainsi une nouvelle application gérée.

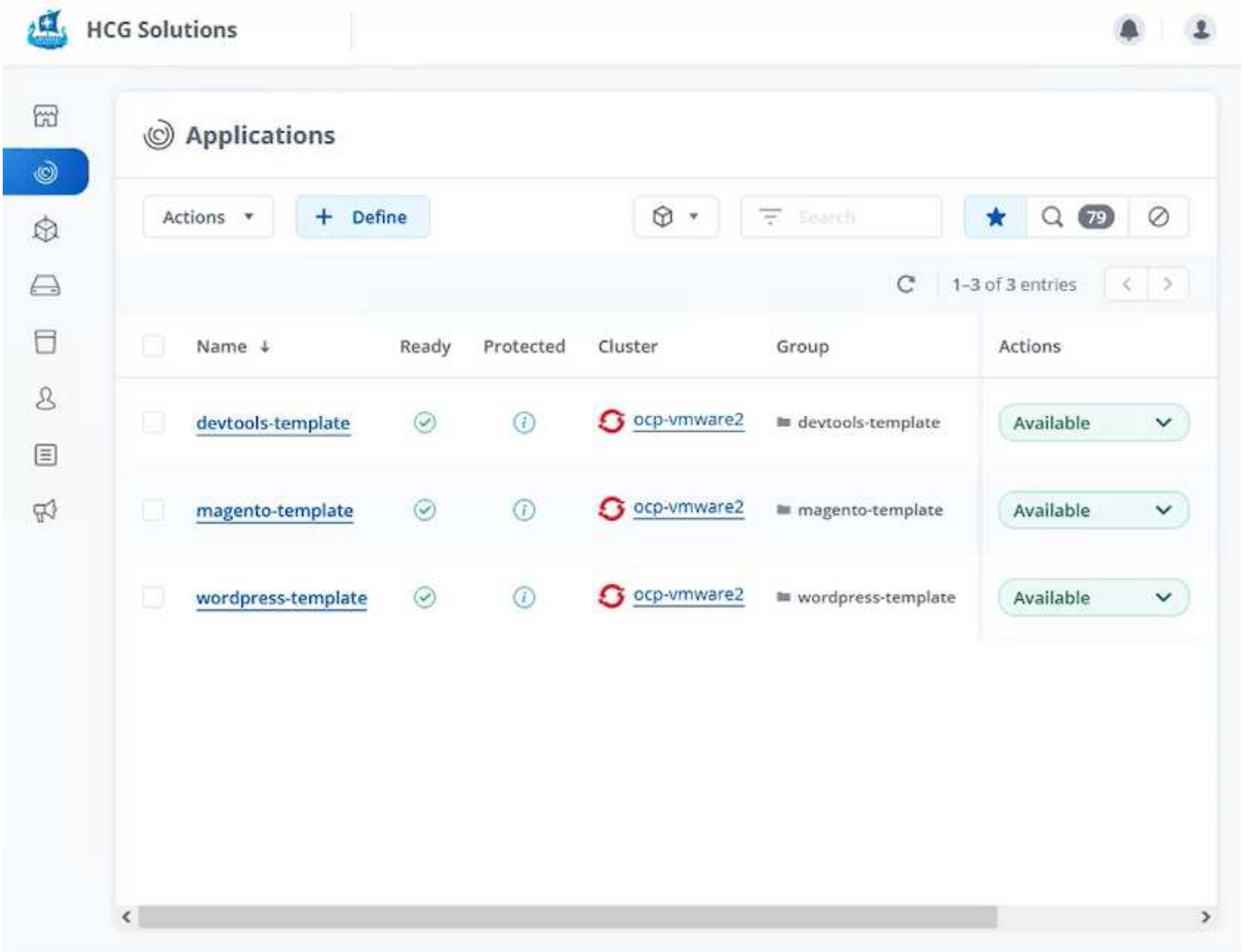
> Cet environnement peut être une seule application autonome en cours de développement ou dans l'ensemble d'un environnement de développement comme un pipeline ci/CD Jenkins.

4. L'utilisateur extrait ensuite une version de son code dans l'environnement de développement cloné à partir d'un référentiel en ligne tel que Gitea.
5. La nouvelle version de l'application est déployée et gérée par NetApp Astra Control.

> Ces deux processus peuvent être automatisés.

6. L'utilisateur peut développer un nouveau code dans cet environnement cloné.
7. Lorsque l'utilisateur est satisfait de ses efforts de développement, il peut renvoyer le code vers le référentiel hébergé.

L'utilisation présentée ici dépend de l'existence de modèles optimisés pour les environnements ou les applications que vous souhaitez cloner. Dans notre environnement, nous avons créé trois de ces modèles, un pour un déploiement Wordpress, un pour un déploiement Magento, et un pour un environnement ci/CD Jenkins avec Gitea que nous avons intitulé DevTools.



Chacun de ces environnements est géré par le contrôle NetApp Astra, avec des volumes persistants stockés sur un système de stockage NetApp ONTAP avec un back-end NFS fourni par NetApp Astra Trident.

Validation du cas d'utilisation

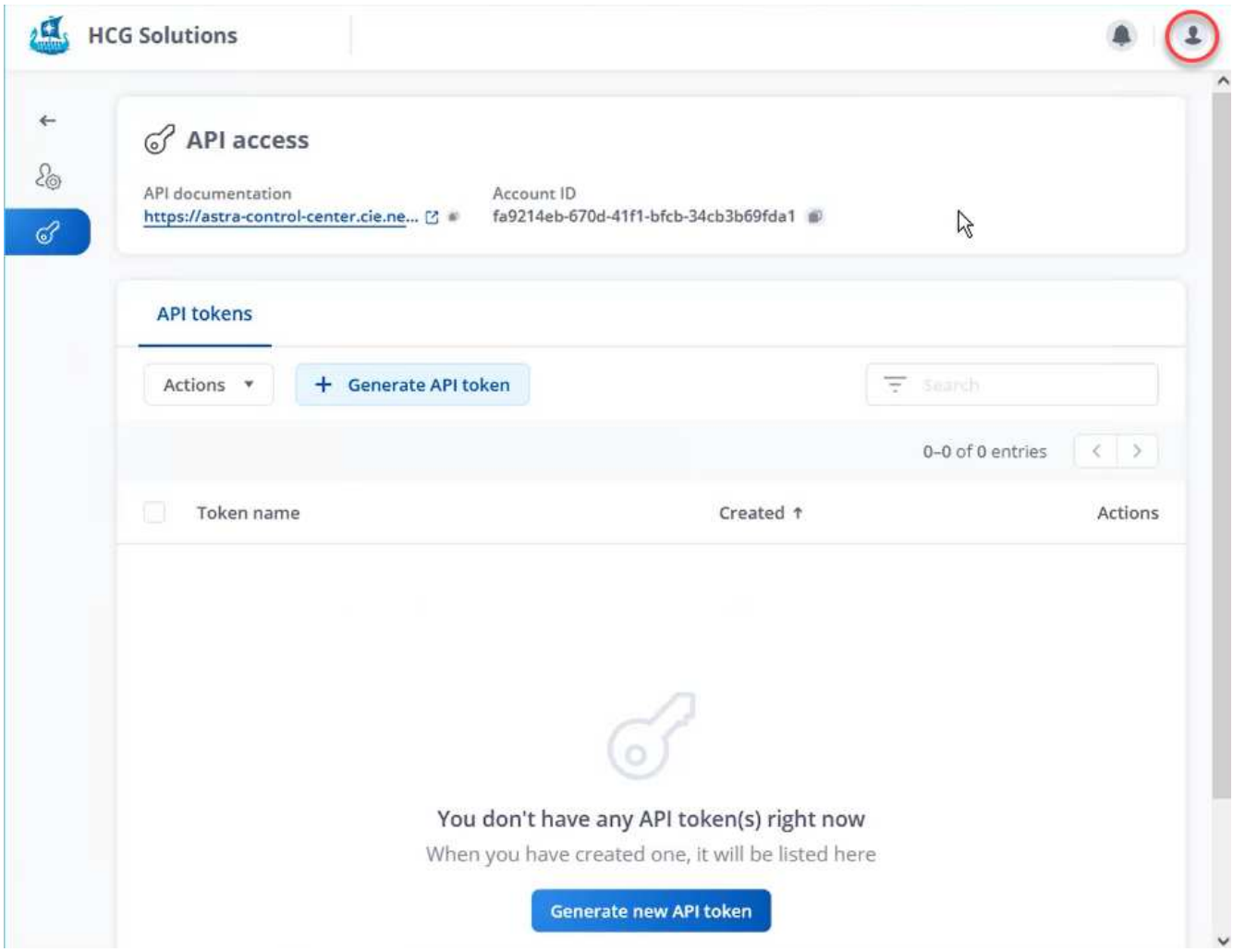
1. Clonez le kit ansible fourni par l'équipe NetApp Solutions Engineering, qui comprend le rôle de clonage et le PlayBook de mise à jour des applications.

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

2. Modifier `vars/clone_vars.yml` Et apportez les valeurs globales adaptées à votre environnement Astra Control.

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

Les valeurs globales d'environnement à remplir sont disponibles sous l'icône de profil utilisateur de NetApp Astra Control, sous le menu d'accès à l'API.



3. Lorsque les variables globales sont terminées, vous pouvez choisir les valeurs de l'application spécifique que vous souhaitez cloner. Pour cloner l'environnement devTools vers un environnement personnel appelé `alan-devtools`, procédez comme suit :

```
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
```

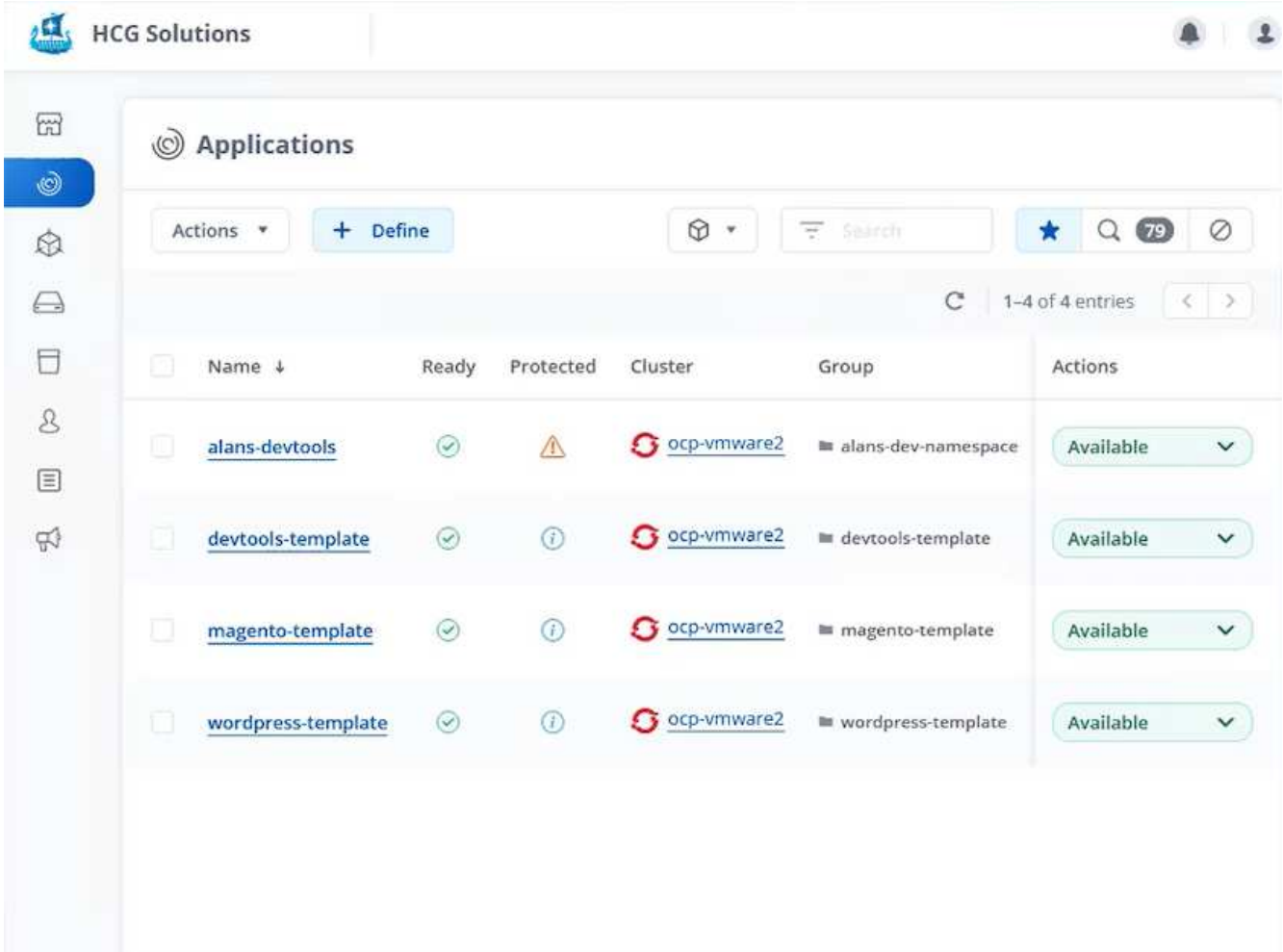
Pour tirer parti de la technologie NetApp FlexClone dans le processus de clonage, `src-cluster` et `dest-cluster` doit être identique.

4. Vous pouvez désormais exécuter le manuel de vente pour cloner l'application.

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

> Le manuel tel qu'écrit doit être exécuté par l'utilisateur root ou par une personne pouvant faire remonter à travers le processus sudo en passant l'argument « -K ».

5. Lorsque le manuel de vente termine son exécution, l'application clonée apparaît comme disponible dans la console Astra Control Center.



6. Un utilisateur peut ensuite se connecter à l'environnement Kubernetes où l'application a été déployée, vérifier que l'application est exposée avec une nouvelle adresse IP, et lancer son travail de développement.

Pour une démonstration de ce cas d'utilisation et un exemple de mise à niveau d'une application, voir "ici".

Vidéos et démonstrations : le DevOps avec NetApp Astra

Les vidéos suivantes présentent certaines des fonctionnalités décrites dans ce document :

Protection des données dans un pipeline ci/CD avec Astra Control Center

Utilisez l'Astra de NetApp pour effectuer une analyse post-mortem et restaurer votre application

Accélérez le développement logiciel avec Astra Control et la technologie NetApp FlexClone

NetApp Astra, avec le DevOps

Pour en savoir plus sur les informations fournies dans ce document, consultez les sites web suivants :

- Documentation NetApp

  "https://docs.netapp.com/"

- Documentation Trident d'Astra

  "https://docs.netapp.com/us-en/trident/"

- Documentation NetApp Astra Control Center

  "https://docs.netapp.com/us-en/astra-control-center/"

- Documentation Ansible

  "https://docs.ansible.com/"

- Documentation Red Hat OpenShift

  "https://access.redhat.com/documentation/en-us/openshift_container_platform/4.8/"

- Documentation de l'éleveur

  "https://rancher.com/docs/"

- Documentation Kubernetes

  "https://kubernetes.io/docs/home/"

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.