Protéger les charges de travail Kubernetes (Aperçu)

NetApp Backup and Recovery

NetApp
October 21, 2025

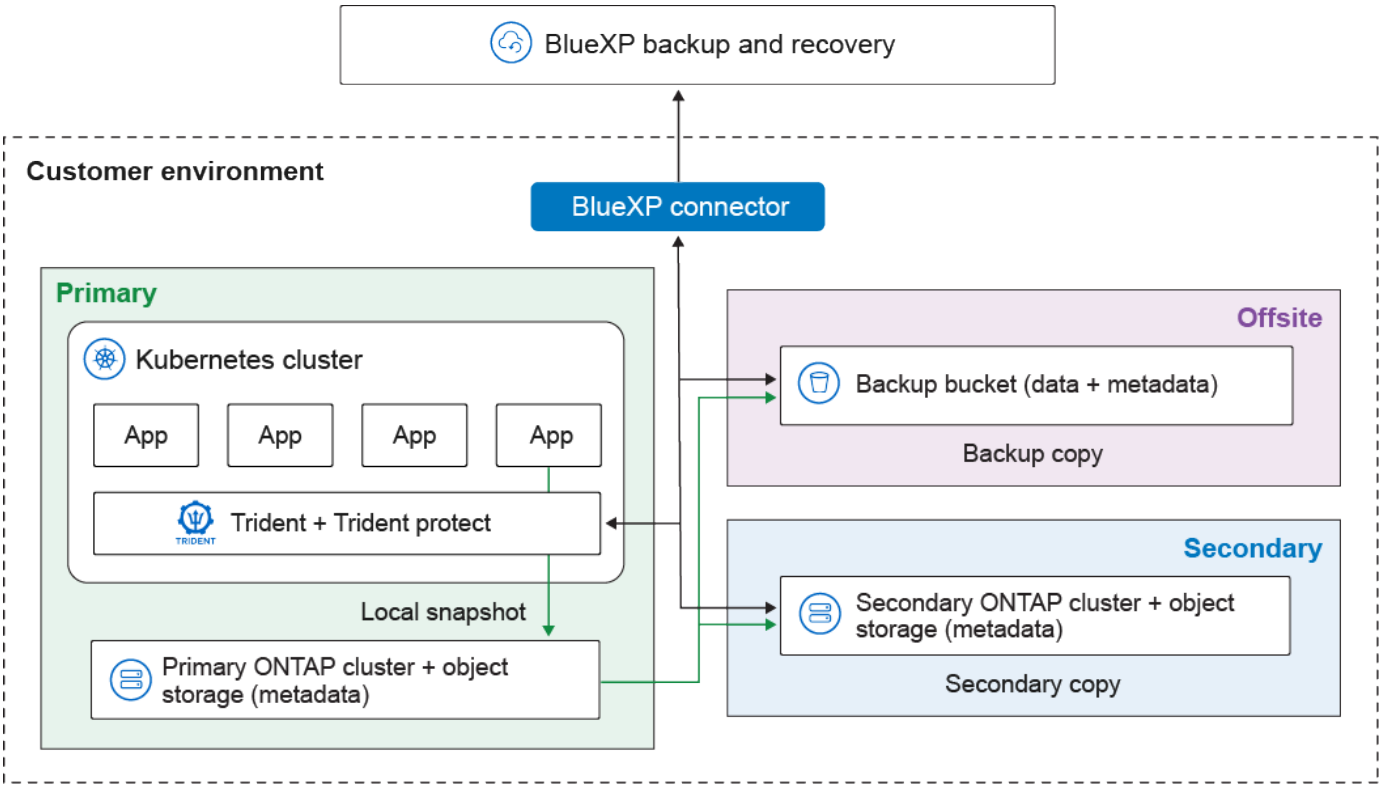
Sommaire

Protéger les charges de travail Kubernetes (Aperçu)

Présentation de la gestion des charges de travail Kubernetes

La gestion des charges de travail Kubernetes dans NetApp Backup and Recovery vous permet de découvrir, de gérer et de protéger vos clusters et applications Kubernetes en un seul endroit. Vous pouvez gérer les ressources et les applications hébergées sur vos clusters Kubernetes. Vous pouvez également créer et associer des politiques de protection à vos charges de travail Kubernetes, le tout depuis une interface unique.

Le diagramme suivant montre les composants et l'architecture de base de la sauvegarde et de la restauration des charges de travail Kubernetes et comment différentes copies de vos données peuvent être stockées à différents emplacements :



NetApp Backup and Recovery offre les avantages suivants pour la gestion des charges de travail Kubernetes :

- Un plan de contrôle unique pour protéger les applications exécutées sur plusieurs clusters Kubernetes. Ces applications peuvent inclure des conteneurs ou des machines virtuelles exécutés sur vos clusters Kubernetes.
- Intégration native avec NetApp SnapMirror, permettant des capacités de déchargement du stockage pour tous les flux de travail de sauvegarde et de récupération.
- Sauvegardes incrémentielles permanentes pour les applications Kubernetes, se traduisant par des objectifs de point de récupération (RPO) et des objectifs de temps de récupération (RTO) inférieurs.

Cette documentation est fournie à titre d'aperçu technologique. Pendant la phase d'aperçu, la fonctionnalité Kubernetes n'est pas recommandée pour les charges de travail de production. Avec cette offre préliminaire, NetApp se réserve le droit de modifier les détails, le contenu et le calendrier de l'offre avant la disponibilité générale.

Vous pouvez effectuer les tâches suivantes liées à la gestion des charges de travail Kubernetes :

- "Découvrez les charges de travail Kubernetes".
- "Gérer les clusters Kubernetes".
- "Ajouter et protéger les applications Kubernetes".
- "Gérer les applications Kubernetes".
- "Restaurer les applications Kubernetes".

Découvrez les charges de travail Kubernetes dans NetApp Backup and Recovery

NetApp Backup and Recovery doit découvrir les charges de travail Kubernetes avant de les protéger.

Rôle de NetApp Console requis Super administrateur de sauvegarde et de récupération. En savoir plus sur"Rôles et privilèges de sauvegarde et de récupération" . "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Découvrez les charges de travail Kubernetes

Dans l'inventaire de sauvegarde et de récupération, découvrez les charges de travail Kubernetes dans votre environnement. L'ajout d'une charge de travail ajoute un cluster Kubernetes à NetApp Backup and Recovery. Vous pouvez ensuite ajouter des applications et protéger les ressources du cluster.

Étapes

1. Effectuez l'une des opérations suivantes :
   - Si vous découvrez des charges de travail Kubernetes pour la première fois, dans NetApp Backup and Recovery, sélectionnez **Découvrir et gérer** sous le type de charge de travail Kubernetes.
   - Si vous avez déjà découvert des charges de travail Kubernetes, dans NetApp Backup and Recovery, sélectionnez **Inventaire** > **Charges de travail**, puis sélectionnez **Découvrir les ressources**.
2. Sélectionnez le type de charge de travail **Kubernetes**.
3. Saisissez un nom de cluster et choisissez un connecteur à utiliser avec le cluster.
4. Suivez les instructions de la ligne de commande qui s'affichent :
   - Créer un espace de noms de protection Trident
   - Créer un secret Kubernetes
   - Ajouter un dépôt Helm
   - Installer Trident Protect et le connecteur Trident Protect

     Ces étapes garantissent que NetApp Backup and Recovery peut interagir avec le cluster.
5. Une fois les étapes terminées, sélectionnez **Découvrir**.

Le cluster est ajouté à l'inventaire.

6. Sélectionnez **Afficher** dans la charge de travail Kubernetes associée pour voir la liste des applications, des clusters et des espaces de noms pour cette charge de travail.

Accéder au tableau de bord de NetApp Backup and Recovery

Suivez ces étapes pour afficher le tableau de bord de NetApp Backup and Recovery .

1. Dans le menu de la NetApp Console , sélectionnez **Protection** > **Sauvegarde et récupération**.
2. Sélectionnez une mosaïque de charge de travail (par exemple, Microsoft SQL Server).
3. Dans le menu Sauvegarde et récupération, sélectionnez **Tableau de bord**.
4. Examiner l'état de santé de la protection des données. Le nombre de charges de travail à risque ou protégées augmente en fonction des charges de travail nouvellement découvertes, protégées et sauvegardées.

   "Découvrez ce que le tableau de bord vous montre".

Ajouter et protéger les applications Kubernetes

NetApp Backup and Recovery vous permet de découvrir facilement vos clusters Kubernetes, sans générer ni télécharger de fichiers kubeconfig. Vous pouvez connecter des clusters Kubernetes et installer le logiciel requis à l'aide de commandes simples copiées à partir de l'interface utilisateur de la NetApp Console .

Rôle de NetApp Console requis

Administrateur d'organisation ou administrateur SnapCenter . "En savoir plus sur les rôles d'accès à NetApp Backup and Recovery" . "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Ajouter et protéger une nouvelle application Kubernetes

La première étape de la protection des applications Kubernetes consiste à créer une application dans NetApp Backup and Recovery. Lorsque vous créez une application, vous informez la console de l'application en cours d'exécution sur le cluster Kubernetes.

Avant de commencer

Avant de pouvoir ajouter et protéger une application Kubernetes, vous devez"découvrir les charges de travail Kubernetes" .

Étapes

1. Dans NetApp Backup and Recovery, sélectionnez **Inventaire**.
2. Choisissez une instance Kubernetes et sélectionnez **Afficher** pour afficher les ressources associées à cette instance.
3. Sélectionnez l'onglet **Applications**.
4. Sélectionnez **Créer une application**.
5. Entrez un nom pour l'application.
6. Vous pouvez également choisir l'un des champs suivants pour rechercher les ressources que vous souhaitez protéger :

- Cluster associé
- Espaces de noms associés
- Types de ressources
- Sélecteurs d'étiquettes

7. Vous pouvez également sélectionner « Ressources à portée de cluster » pour choisir les ressources à portée de cluster. Si vous les incluez, elles seront ajoutées à l'application lors de sa création.
8. Vous pouvez également sélectionner **Rechercher** pour trouver les ressources en fonction de vos critères de recherche.

> La console ne stocke pas les paramètres ou les résultats de recherche ; les paramètres sont utilisés pour rechercher dans le cluster Kubernetes sélectionné des ressources pouvant être incluses dans l'application.

9. La console affiche une liste de ressources correspondant à vos critères de recherche.
10. Si la liste contient les ressources que vous souhaitez protéger, sélectionnez **Suivant**.
11. Vous pouvez également, dans la zone **Politique**, choisir une politique de protection existante pour protéger l'application ou en créer une nouvelle. Si vous ne sélectionnez pas de politique, l'application est créée sans politique de protection. Tu peux"ajouter une politique de protection" plus tard.
12. Dans la zone **Préscripts et postscripts**, activez et configurez tous les hooks d'exécution de préscripts ou de postscripts que vous souhaitez exécuter avant ou après les opérations de sauvegarde. Pour activer les prescripts ou les postscripts, vous devez déjà en avoir créé au moins un"modèle de crochet d'exécution" .
13. Sélectionnez **Créer**.

Résultat

L'application est créée et apparaît dans la liste des applications dans l'onglet **Applications** de l'inventaire Kubernetes. La NetApp Console active la protection de l'application en fonction de vos paramètres et vous pouvez surveiller la progression dans la zone **Surveillance** de la sauvegarde et de la récupération.

Protéger une application Kubernetes existante

Activez une politique de protection sur une application Kubernetes que vous avez déjà ajoutée.

Étapes

1. Dans NetApp Backup and Recovery, sélectionnez **Inventaire**.
2. Choisissez une instance Kubernetes et sélectionnez **Afficher** pour afficher les ressources associées à cette instance.
3. Sélectionnez l'onglet **Applications**.
4. Dans la liste des applications, choisissez une application que vous souhaitez protéger et sélectionnez le menu Actions associé.
5. Sélectionnez **Protéger**.
6. Dans la zone **Politique**, choisissez une politique de protection existante pour protéger l'application ou créez une nouvelle politique. Se référer à"Créer une politique" pour plus d'informations sur la création de politiques de protection.
7. Dans la zone **Préscripts et postscripts**, activez et configurez tous les hooks d'exécution de préscripts ou de postscripts que vous souhaitez exécuter avant ou après les opérations de sauvegarde. Vous pouvez configurer le type de hook d'exécution, le modèle qu'il utilise, les arguments et les sélecteurs d'étiquettes.

8. Sélectionnez **Terminé**.

Résultat

La console active la protection de l'application en fonction de vos paramètres et vous pouvez surveiller la progression dans la zone **Surveillance** de la sauvegarde et de la récupération. Dès que vous activez la protection d'une application, la console crée une sauvegarde complète de l'application. Les sauvegardes incrémentielles ultérieures sont créées selon la planification définie dans la politique de protection associée à l'application.

Sauvegarder une application Kubernetes maintenant

Créez manuellement une sauvegarde d'une application Kubernetes pour établir une base de référence pour les futures sauvegardes et instantanés, ou pour garantir la protection des données les plus récentes.

Étapes

1. Dans NetApp Backup and Recovery, sélectionnez **Inventaire**.
2. Choisissez une instance Kubernetes et sélectionnez **Afficher** pour afficher les ressources associées à cette instance.
3. Sélectionnez l'onglet **Applications**.
4. Dans la liste des applications, choisissez une application que vous souhaitez sauvegarder et sélectionnez le menu Actions associé.
5. Sélectionnez **Sauvegarder maintenant**.
6. Assurez-vous que le nom d'application correct est sélectionné.
7. Sélectionnez **Sauvegarder**.

Résultat

La console crée une sauvegarde de l'application et affiche la progression dans la zone **Surveillance** de Sauvegarde et récupération. La sauvegarde est créée en fonction de la politique de protection associée à l'application.

Restaurer les applications Kubernetes

NetApp Backup and Recovery vous permet de restaurer les applications que vous avez protégées avec une politique de protection. Pour restaurer une application, celle-ci doit disposer d'au moins un point de restauration. Un point de restauration est constitué soit de l'instantané local, soit de la sauvegarde dans le magasin d'objets (ou des deux). Vous pouvez restaurer une application à partir de l'archive locale, secondaire ou du magasin d'objets.

Rôle de NetApp Console requis

Administrateur d'organisation ou administrateur SnapCenter . "En savoir plus sur les rôles d'accès à NetApp Backup and Recovery" . "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Étapes

1. Dans NetApp Backup and Recovery, sélectionnez **Inventaire**.
2. Choisissez une instance Kubernetes et sélectionnez **Afficher** pour afficher les ressources associées à cette instance.

3. Sélectionnez l'onglet **Applications**.
4. Dans la liste des applications, choisissez une application que vous souhaitez restaurer et sélectionnez le menu Actions associé.
5. Sélectionnez **Afficher et restaurer**.

   La liste des points de restauration apparaît.

6. Ouvrez le menu Actions pour le point de restauration que vous souhaitez utiliser et sélectionnez **Restaurer**.

Paramètres généraux

1. Choisissez la source à partir de laquelle restaurer (local ou magasin d'objets).
2. Choisissez le cluster de destination dans la liste **Cluster**.
3. Choisissez l'espace de noms de destination de restauration.

   Vous pouvez restaurer l'espace de noms d'origine ou restaurer un nouvel espace de noms.

4. Sélectionnez **Suivant**.

Sélection des ressources

1. Choisissez si vous souhaitez restaurer toutes les ressources associées à l'application ou utiliser un filtre pour sélectionner des ressources spécifiques à restaurer :

Restaurer toutes les ressources

1. Sélectionnez **Restaurer toutes les ressources**.
2. Sélectionnez **Suivant**.

Restaurer des ressources spécifiques

1. Sélectionnez **Ressources sélectives**.
2. Choisissez le comportement du filtre de ressources. Si vous choisissez **Inclure**, les ressources que vous sélectionnez sont restaurées. Si vous choisissez **Exclure**, les ressources que vous sélectionnez ne sont pas restaurées.
3. Sélectionnez **Ajouter des règles** pour ajouter des règles qui définissent des filtres pour la sélection des ressources. Vous avez besoin d'au moins une règle pour filtrer les ressources.

   Chaque règle peut filtrer selon des critères tels que l'espace de noms de la ressource, les étiquettes, le groupe, la version et le type.

4. Sélectionnez **Enregistrer** pour enregistrer chaque règle.
5. Lorsque vous avez ajouté toutes les règles dont vous avez besoin, sélectionnez **Rechercher** pour voir les ressources disponibles dans l'archive de sauvegarde qui correspondent à vos critères de filtre.

   Les ressources affichées sont les ressources qui existent actuellement sur le cluster.

6. Lorsque vous êtes satisfait des résultats, sélectionnez **Suivant**.

Paramètres de destination

1. Choisissez de restaurer soit la classe de stockage par défaut, soit une classe de stockage différente.
2. Si vous choisissez de restaurer vers une classe de stockage différente, sélectionnez une classe de stockage de destination correspondant à chaque classe de stockage source.
3. Sélectionnez **Restaurer**.

Gérer les clusters Kubernetes

NetApp Backup and Recovery vous permet de découvrir et de gérer vos clusters Kubernetes afin de protéger les ressources hébergées par les clusters.

Rôle de NetApp Console requis

Administrateur d'organisation ou administrateur SnapCenter . "En savoir plus sur les rôles d'accès à NetApp Backup and Recovery" . "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Pour découvrir les clusters Kubernetes, reportez-vous à"Découvrez les charges de travail Kubernetes" .

Modifier les informations du cluster Kubernetes

Vous pouvez modifier un cluster si vous devez changer son nom.

Étapes

1. Dans NetApp Backup and Recovery, sélectionnez **Inventaire** > **Clusters**.
2. Dans la liste des clusters, choisissez un cluster que vous souhaitez modifier et sélectionnez le menu Actions associé.
3. Sélectionnez **Modifier le cluster**.
4. Apportez les modifications nécessaires au nom du cluster. Ce nom doit correspondre à celui utilisé avec la commande Helm lors de la découverte.
5. Sélectionnez **Terminé**.

Supprimer un cluster Kubernetes

Pour arrêter la protection d'un cluster Kubernetes, désactivez la protection et supprimez les applications associées, puis supprimez le cluster de NetApp Backup and Recovery. NetApp Backup and Recovery ne supprime pas le cluster ni ses ressources ; il supprime uniquement le cluster de l'inventaire de la NetApp Console .

Étapes

1. Dans NetApp Backup and Recovery, sélectionnez **Inventaire** > **Clusters**.
2. Dans la liste des clusters, choisissez un cluster que vous souhaitez modifier et sélectionnez le menu Actions associé.
3. Sélectionnez **Supprimer le cluster**.
4. Vérifiez les informations dans la boîte de dialogue de confirmation et sélectionnez **Supprimer**.

Gérer les applications Kubernetes

NetApp Backup and Recovery vous permet de déprotéger et de supprimer vos applications Kubernetes et les ressources associées.

Rôle de NetApp Console requis

Administrateur d'organisation ou administrateur SnapCenter . "En savoir plus sur les rôles d'accès à NetApp Backup and Recovery" . "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Déprotéger une application Kubernetes

Vous pouvez déprotéger une application si vous ne souhaitez plus la protéger. Lorsque vous déprotégez une application, NetApp Backup and Recovery cesse de protéger l'application mais conserve toutes les sauvegardes et tous les snapshots associés.

Étapes

1. Dans NetApp Backup and Recovery, sélectionnez **Inventaire**.
2. Choisissez une instance Kubernetes et sélectionnez **Afficher** pour afficher les ressources associées à cette instance.
3. Sélectionnez l'onglet **Applications**.
4. Dans la liste des applications, choisissez une application que vous souhaitez déprotéger et sélectionnez le menu Actions associé.
5. Sélectionnez **Déprotéger**.
6. Lisez l'avis et, lorsque vous êtes prêt, sélectionnez **Déprotéger**.

Supprimer une application Kubernetes

Supprimez une application dont vous n'avez plus besoin. NetApp Backup and Recovery arrête la protection et supprime toutes les sauvegardes et tous les instantanés des applications supprimées.

Étapes

1. Dans NetApp Backup and Recovery, sélectionnez **Inventaire**.
2. Choisissez une instance Kubernetes et sélectionnez **Afficher** pour afficher les ressources associées à cette instance.
3. Sélectionnez l'onglet **Applications**.
4. Dans la liste des applications, choisissez une application que vous souhaitez supprimer et sélectionnez le menu Actions associé.
5. Sélectionnez **Supprimer**.
6. Activez **Supprimer les instantanés et les sauvegardes** pour supprimer tous les instantanés et sauvegardes de l'application.

   Vous ne pourrez plus restaurer l'application à l'aide de ces instantanés et sauvegardes.

7. Confirmez l'action et sélectionnez **Supprimer**.

Gérer les modèles de hook d’exécution de NetApp Backup and Recovery pour les charges de travail Kubernetes

Un hook d’exécution est une action personnalisée qui s’exécute avec une opération de protection des données dans une application Kubernetes gérée. Par exemple, créez des instantanés cohérents avec l’application en utilisant un hook d’exécution pour suspendre les transactions de base de données avant un instantané et les reprendre après. Lorsque vous créez un modèle de hook d’exécution, spécifiez le type de hook, le script à exécuter et les filtres pour les conteneurs cibles. Utilisez le modèle pour lier les hooks d’exécution à vos applications.

NetApp Backup and Recovery gèle et débloque les systèmes de fichiers pour des applications comme KubeVirt pendant la protection des données. Vous pouvez désactiver ce comportement globalement ou pour des applications spécifiques à l’aide de la documentation Trident Protect :

- Pour désactiver ce comportement pour toutes les applications, reportez-vous à "Protection des données avec les machines virtuelles KubeVirt" .
- Pour désactiver ce comportement pour une application spécifique, reportez-vous à "Définir une application" .

Rôle de NetApp Console requis

Administrateur d’organisation ou administrateur SnapCenter . "En savoir plus sur les rôles d’accès à NetApp Backup and Recovery" . "En savoir plus sur les rôles d’accès à la NetApp Console pour tous les services" .

Types de hooks d’exécution

NetApp Backup and Recovery prend en charge les types de hooks d’exécution suivants, en fonction du moment où ils peuvent être exécutés :

- Pré-instantané
- Post-instantané
- Pré-sauvegarde
- Post-sauvegarde
- Post-restauration

Ordre d’exécution

Lorsqu’une opération de protection des données est exécutée, les événements de hook d’exécution se produisent dans l’ordre suivant :

1. Tous les hooks d’exécution de pré-opération personnalisés applicables sont exécutés sur les conteneurs appropriés. Vous pouvez créer plusieurs hooks de pré-opération personnalisés, mais leur ordre d’exécution n’est ni garanti ni configurable.
2. Des blocages du système de fichiers se produisent, le cas échéant.
3. L’opération de protection des données est effectuée.
4. Les systèmes de fichiers gelés sont dégelés, le cas échéant.
5. NetApp Backup and Recovery exécute tous les hooks d’exécution de pré-opération personnalisés

applicables sur les conteneurs appropriés. Vous pouvez créer plusieurs hooks post-opération personnalisés, mais leur ordre d'exécution n'est ni garanti ni configurable.

Si vous créez plusieurs hooks du même type, leur ordre d'exécution n'est pas garanti. Les crochets de différents types fonctionnent toujours dans l'ordre spécifié. Par exemple, voici l'ordre d'exécution d'une configuration qui possède tous les différents types de hooks :

1. Hooks pré-instantanés exécutés
2. Hooks post-instantanés exécutés
3. Hooks de pré-sauvegarde exécutés
4. Hooks post-sauvegarde exécutés

Testez les scripts d'exécution avant de les activer en production. Utilisez « kubectl exec » pour tester les scripts, puis vérifiez les instantanés et les sauvegardes en clonant l'application dans un espace de noms temporaire et en la restaurant.

Si un hook d'exécution pré-snapshot ajoute, modifie ou supprime des ressources Kubernetes, ces modifications sont incluses dans le snapshot ou la sauvegarde et dans toute opération de restauration ultérieure.

Remarques importantes sur les hooks d'exécution personnalisés

Tenez compte des éléments suivants lors de la planification des hooks d'exécution pour vos applications.

- Un hook d'exécution doit utiliser un script pour effectuer des actions. De nombreux hooks d'exécution peuvent référencer le même script.
- Les hooks d'exécution doivent être écrits au format de scripts shell exécutables.
- La taille du script est limitée à 96 Ko.
- Les paramètres de hook d'exécution et tous les critères de correspondance sont utilisés pour déterminer quels hooks sont applicables à une opération de snapshot, de sauvegarde ou de restauration.

Les hooks d'exécution peuvent réduire ou désactiver les fonctionnalités de l'application. Faites fonctionner vos crochets personnalisés le plus rapidement possible. Si vous démarrez une opération de sauvegarde ou de snapshot avec des hooks d'exécution associés, mais que vous l'annulez ensuite, les hooks sont toujours autorisés à s'exécuter si l'opération de sauvegarde ou de snapshot a déjà commencé. Cela signifie que la logique utilisée dans un hook d'exécution post-sauvegarde ne peut pas supposer que la sauvegarde a été terminée.

Filtres de crochet d'exécution

Lorsque vous ajoutez ou modifiez un hook d'exécution pour une application, vous pouvez ajouter des filtres au hook d'exécution pour gérer les conteneurs auxquels le hook correspondra. Les filtres sont utiles pour les applications qui utilisent la même image de conteneur sur tous les conteneurs, mais peuvent utiliser chaque image à des fins différentes (comme Elasticsearch). Les filtres vous permettent de créer des scénarios dans lesquels les hooks d'exécution s'exécutent sur certains conteneurs identiques, mais pas nécessairement sur tous. Si vous créez plusieurs filtres pour un seul hook d'exécution, ils sont combinés avec un opérateur AND logique. Vous pouvez avoir jusqu'à 10 filtres actifs par hook d'exécution.

Chaque filtre que vous ajoutez à un hook d'exécution utilise une expression régulière pour faire correspondre les conteneurs de votre cluster. Lorsqu'un hook correspond à un conteneur, le hook exécutera son script

associé sur ce conteneur. Les expressions régulières pour les filtres utilisent la syntaxe d'expression régulière 2 (RE2), qui ne prend pas en charge la création d'un filtre excluant les conteneurs de la liste des correspondances. Pour plus d'informations sur la syntaxe prise en charge par NetApp Backup and Recovery pour les expressions régulières dans les filtres de hook d'exécution, consultez "Prise en charge de la syntaxe des expressions régulières 2 (RE2)" .

> Si vous ajoutez un filtre d'espace de noms à un hook d'exécution qui s'exécute après une opération de restauration ou de clonage et que la source et la destination de restauration ou de clonage se trouvent dans des espaces de noms différents, le filtre d'espace de noms est appliqué uniquement à l'espace de noms de destination.

Exemples de crochets d'exécution

Visitez le "Projet GitHub NetApp Verda" pour télécharger de véritables hooks d'exécution pour des applications populaires telles qu'Apache Cassandra et Elasticsearch. Vous pouvez également voir des exemples et obtenir des idées pour structurer vos propres hooks d'exécution personnalisés.

Créer un modèle de hook d'exécution

Vous pouvez créer un modèle de hook d'exécution personnalisé que vous pouvez utiliser pour effectuer des actions avant ou après une opération de protection des données sur une application.

Étapes

1. Dans la console, accédez à **Protection** > **Sauvegarde et récupération**.
2. Sélectionnez l'onglet **Paramètres**.
3. Développez la section **Modèle de hook d'exécution**.
4. Sélectionnez **Créer un modèle de hook d'exécution**.
5. Entrez un nom pour le hook d'exécution.
6. Vous pouvez également choisir un type de hook. Par exemple, un hook post-restauration est exécuté une fois l'opération de restauration terminée.
7. Dans la zone de texte **Script**, saisissez le script shell exécutable que vous souhaitez exécuter dans le cadre du modèle de hook d'exécution. Vous pouvez également sélectionner **Télécharger le script** pour télécharger un fichier de script à la place.
8. Sélectionnez **Créer**.

   Une fois le modèle créé, il apparaît dans la liste des modèles dans la section **Modèle de hook d'exécution**.

Informations sur le copyright

Informations sur les marques commerciales