Notes de mise à jour

Astra Control Center

NetApp
March 12, 2024

Sommaire

Notes de mise à jour

Nous sommes heureux d'annoncer la dernière version d'Astra Control Center.

- "Dans cette version d'Astra Control Center"
- "Problèmes connus"
- "Limites connues"

Envoyez vos commentaires sur la documentation en devenant un "Contributeur GitHub" ou en envoyant un e-mail à doccomments@netapp.com.

Nouveautés de la nouvelle version d'Astra Control Center

Nous sommes heureux d'annoncer la dernière version d'Astra Control Center.

7 novembre 2023 (23.10.0)

Nouvelles fonctionnalités et prises en charge

- **Fonctionnalités de sauvegarde et de restauration pour les applications avec les systèmes back-end de stockage ontap-nas économiques à base de pilotes** : activez les opérations de sauvegarde et de restauration `ontap-nas-economy` avec certains "étapes simples".
- **Sauvegardes immuables** : Astra Control prend désormais en charge "sauvegardes inaltérables et en lecture seule" en tant que couche de sécurité supplémentaire contre les programmes malveillants et autres menaces.
- **Présentation d'Astra Control provisionner**

  Avec la version 23.10, Astra Control présente un nouveau composant logiciel appelé Astra Control Provisioner qui sera disponible pour tous les utilisateurs d'Astra Control sous licence. ASTRA Control Provisioner offre un accès à un ensemble complet de fonctionnalités de gestion et de provisionnement du stockage avancées qui vont au-delà de celles d'Astra Trident. Ces fonctionnalités sont disponibles sans frais supplémentaires pour tous les clients d'Astra Control.

  - **Commencez avec Astra Control Provisioner**
    C'est possible "Activez le mécanisme de provisionnement Astra Control" Si vous avez installé et configuré votre environnement pour utiliser Astra Trident 23.10.
  - **Fonctionnalité Astra Control Provisioner**

    Les fonctions suivantes sont disponibles avec l'Astra Control Provisioner 23.10 :

    - **Sécurité renforcée du back-end de stockage avec le cryptage Kerberos 5** : vous pouvez améliorer la sécurité du stockage par "activation du chiffrement" pour le trafic entre votre cluster géré et le back-end de stockage. ASTRA Control Provisioner prend en charge le chiffrement Kerberos 5 sur connexions NFSv4.1 des clusters Red Hat OpenShift aux volumes Azure NetApp Files et ONTAP sur site
    - **Récupérer des données à l'aide d'un snapshot** : Astra Control provisionner offre une restauration rapide de volume sur place à partir d'un snapshot à l'aide du `TridentActionSnapshotRestore` (TASR) CR.
    - **Améliorations de SnapMirror** : utilisez la fonctionnalité de réplication d'applications dans les environnements où Astra Control ne dispose pas d'une connectivité directe à un cluster ONTAP ou

d'un accès aux informations d'identification ONTAP. Cette fonctionnalité vous permet d'utiliser la réplication sans devoir gérer un système back-end de stockage ou ses identifiants dans Astra Control.

    - **Fonctionnalités de sauvegarde et de restauration pour les applications avec `ontap-nas-economy` Systèmes back-end avec sauvegarde par pilote** : comme décrit ci-dessus.

- **Prise en charge de la gestion des applications qui utilisent le stockage NVMe/TCP**
  ASTRA Control peut désormais gérer des applications sauvegardées par des volumes persistants et connectés via NVMe/TCP.
- **Crochets d'exécution désactivés par défaut** : à partir de cette version, la fonctionnalité crochets d'exécution peut être "activé" ou désactivé pour une sécurité supplémentaire (il est désactivé par défaut). Si vous n'avez pas encore créé de crochets d'exécution pour une utilisation avec Astra Control, vous devez le faire "activez la fonction crochets d'exécution" pour commencer à créer des crochets. Si vous avez créé des crochets d'exécution avant cette version, la fonctionnalité crochets d'exécution reste activée et vous pouvez utiliser des crochets comme vous le feriez normalement.

Problèmes et limites connus

- "Problèmes connus pour cette version"
- "Restrictions connues pour cette version"

31 juillet 2023 (23.07.0)

Détails

Nouvelles fonctionnalités et prises en charge

- "Prise en charge de l'utilisation de NetApp MetroCluster dans une configuration étendue en tant que back-end de stockage"
- "Prise en charge de l'utilisation de Longhorn en tant que système back-end de stockage"
- "Il est désormais possible de répliquer des applications entre des systèmes ONTAP back-end à partir du même cluster Kubernetes"
- "ASTRA Control Center prend désormais en charge « userPrincipalName » en tant qu'attribut de connexion alternatif pour les utilisateurs distants (LDAP)"
- "Un nouveau type de crochet d'exécution « post-basculement » peut être exécuté après le basculement de réplication avec Astra Control Center"
- Les workflows de clonage ne prennent désormais en charge que les clones dynamiques (état actuel de l'application gérée). Pour cloner à partir d'un snapshot ou d'une sauvegarde, utilisez "restaurer le flux de travail".

Problèmes et limites connus

- "Problèmes connus pour cette version"
- "Restrictions connues pour cette version"

18 mai 2023 (23.04.2)

Détails

Ce correctif (23.04.2) pour Astra Control Center (23.04.0) prend en charge "Plug-in externe Kubernetes CSI v6.1.0" et corrige les problèmes suivants :

- Bogue avec la restauration d'applications sur place lors de l'utilisation de hooks d'exécution
- Problèmes de connexion avec le service de godet

25 avril 2023 (23.04.0)

Détails

Nouvelles fonctionnalités et prises en charge

- "Licence d'évaluation de 90 jours activée par défaut pour les nouvelles installations d'Astra Control Center"
- "Fonctionnalité améliorée de crochets d'exécution avec options de filtrage supplémentaires"
- "Les crochets d'exécution peuvent maintenant être exécutés après le basculement de la réplication avec Astra Control Center"
- "Prise en charge de la migration des volumes de la classe de stockage « ONTAP-nas-Economy » vers la classe de stockage « ontap-nas »"
- "Prise en charge de l'inclusion ou de l'exclusion des ressources applicatives pendant les opérations de restauration"
- "Prise en charge de la gestion des applications données uniquement"

Problèmes et limites connus

- "Problèmes connus pour cette version"
- "Restrictions connues pour cette version"

22 novembre 2022 (22.11.0)

Détails

Nouvelles fonctionnalités et prises en charge

- "Prise en charge des applications réparties sur plusieurs espaces de noms"
- "La prise en charge de l'inclusion des ressources de cluster dans une définition d'application"
- "L'authentification LDAP optimisée avec l'intégration du contrôle d'accès basé sur des rôles (RBAC)"
- "Ajout de la prise en charge de Kubernetes 1.25 et de Pod Security admission (PSA)"
- "Création de rapports d'avancement pour les opérations de sauvegarde, de restauration et de clonage"

Problèmes et limites connus

- "Problèmes connus pour cette version"
- "Restrictions connues pour cette version"

8 septembre 2022 (22.08.1)

Détails

Cette version (22.08.1) pour Astra Control Center (22.08.0) corrige les bugs mineurs dans la réplication d'applications à l'aide de NetApp SnapMirror.

10 août 2022 (22.08.0)

Détails

Nouvelles fonctionnalités et prises en charge

- "Réplication d'applications à l'aide de la technologie NetApp SnapMirror"
- "Workflow de gestion des applications amélioré"
- "Fonctionnalité améliorée de crochets d'exécution"

> Les crochets d'exécution par défaut avant ou après snapshot de NetApp ont été retirés pour des applications spécifiques dans cette version. Si vous effectuez une mise à niveau vers cette version et que vous ne fournissez pas vos propres crochets d'exécution pour les instantanés, Astra Control ne prendra que des instantanés cohérents avec les collisions. Consultez le "NetApp Verda" Référentiel GitHub pour des exemples de scripts de hook d'exécution que vous pouvez modifier en fonction de votre environnement.

- "Prise en charge de VMware Tanzu Kubernetes Grid Integrated Edition (TKGI)"
- "Prise en charge de Google Anthos"
- "Configuration LDAP (via l'API de contrôle Astra)"

Problèmes et limites connus

- "Problèmes connus pour cette version"
- "Restrictions connues pour cette version"

26 avril 2022 (22.04.0)

Détails

Nouvelles fonctionnalités et prises en charge

- "Contrôle d'accès basé sur des rôles (RBAC) dans un espace de noms"
- "Prise en charge de Cloud Volumes ONTAP"
- "Activation d'entrée générique pour le centre de contrôle Astra"
- "Dépose du godet de l'Astra Control"
- "Prise en charge de la gamme VMware Tanzu"

Problèmes et limites connus

- "Problèmes connus pour cette version"
- "Restrictions connues pour cette version"

14 décembre 2021 (21.12)

Détails

Nouvelles fonctionnalités et prises en charge

- "Restauration des applications"
- "Crochets d'exécution"
- "Prise en charge des applications déployées avec des opérateurs du système namespace"
- "Prise en charge supplémentaire de Kubernetes et Rancher en amont"
- "Mises à niveau d'Astra Control Center"
- "Option Red Hat OperatorHub pour l'installation"

Résolution des problèmes

- "Problèmes résolus pour cette version"

Problèmes et limites connus

- "Problèmes connus pour cette version"
- "Restrictions connues pour cette version"

5 août 2021 (21.08)

Détails

Lancement initial du centre de contrôle Astra.

- "Ce qu'il est"
- "Analysez l'architecture et les composants"
- "Commencez dès maintenant"
- "Installer" et "configuration"
- "Gérez" et "protéger" en applications
- "Gestion des compartiments" et "systèmes back-end"
- "Gestion des comptes"
- "Automatisez votre système avec des API"

Trouvez plus d'informations

- "Problèmes connus pour cette version"
- "Restrictions connues pour cette version"
- "Versions antérieures de la documentation Astra Control Center"

Problèmes connus

Les problèmes connus identifient les problèmes susceptibles de vous empêcher d'utiliser cette version du produit avec succès.

Les problèmes connus suivants ont une incidence sur la version actuelle :

- Les sauvegardes d'applications et les snapshots échouent si la classe volumesnapshotclass est ajoutée après la gestion d'un cluster
- La gestion d'un cluster avec Astra Control Center échoue lorsque le fichier kubeconfig contient plusieurs contextes
- Un pod de surveillance peut se bloquer dans les environnements Istio
- Les opérations de gestion des données d'application échouent avec l'erreur de service interne (500) lorsque Astra Trident est hors ligne
- Les opérations de restauration sur place pour les classes de stockage ontap-nas échouent
- La restauration à partir d'une sauvegarde lors de l'utilisation du chiffrement à la volée Kerberos peut échouer
- Les données de sauvegarde restent dans le compartiment après leur suppression pour les compartiments dont la règle de conservation a expiré

Les sauvegardes d'applications et les snapshots échouent si la classe volumesnapshotclass est ajoutée après la gestion d'un cluster

Les sauvegardes et les snapshots échouent avec un `UI 500 error` dans ce scénario. Pour contourner ce problème, actualisez la liste des applications.

La gestion d'un cluster avec Astra Control Center échoue lorsque le fichier kubeconfig contient plusieurs contextes

Vous ne pouvez pas utiliser un kubeconfig avec plus d'un cluster et un contexte. Voir la "article de la base de connaissances" pour en savoir plus.

Un pod de surveillance peut se bloquer dans les environnements Istio

Si vous couplez Astra Control Center avec Cloud Insights dans un environnement Istio, le `telegraf-rs` le pod peut se bloquer. Pour résoudre ce problème, procédez comme suit :

1. Trouvez le pod qui s'est écrasé :

   ```
   kubectl -n netapp-monitoring get pod | grep Error
   ```

   Vous devez voir les résultats similaires à ce qui suit :

   ```
   NAME READY STATUS RESTARTS AGE
   telegraf-rs-fhhrh 1/2 Error 2 (26s ago) 32s
   ```

2. Redémarrez le module en panne, en le remplaçant `<pod_name_from_output>` avec le nom du pod affecté :

   ```
   kubectl -n netapp-monitoring delete pod <pod_name_from_output>
   ```

   Vous devez voir les résultats similaires à ce qui suit :

   ```
   pod "telegraf-rs-fhhrh" deleted
   ```

3. Vérifiez que le pod a redémarré et qu'il n'est pas dans un état d'erreur :

   ```
   kubectl -n netapp-monitoring get pod
   ```

   Vous devez voir les résultats similaires à ce qui suit :

   ```
   NAME READY STATUS RESTARTS AGE
   telegraf-rs-rrnsb 2/2 Running 0 11s
   ```

Les opérations de gestion des données d'application échouent avec l'erreur de service interne (500) lorsque Astra Trident est hors ligne

Si Astra Trident sur un cluster d'application est mis hors ligne (et reconnecté) et 500 erreurs de service

internes sont rencontrées lors de la tentative de gestion des données d'application, redémarrez tous les nœuds Kubernetes du cluster d'application pour restaurer la fonctionnalité.

Les opérations de restauration sur place pour les classes de stockage ontap-nas échouent

Si vous effectuez une restauration sur place d'une application (restaurez-la dans son espace de noms d'origine) et que la classe de stockage de l'application utilise le `ontap-nas-economy` pilote, l'opération de restauration peut échouer si le répertoire de snapshot n'est pas masqué. Avant de remettre le produit en place, suivez les instructions de la section "Sauvegardez et restaurez les opérations ontap-nas" pour masquer le répertoire d'instantanés.

La restauration à partir d'une sauvegarde lors de l'utilisation du chiffrement à la volée Kerberos peut échouer

Lorsque vous restaurez une application à partir d'une sauvegarde vers un back-end de stockage utilisant le chiffrement à la volée Kerberos, l'opération de restauration peut échouer. Ce problème n'affecte pas la restauration à partir d'un snapshot ni la réplication des données d'application à l'aide de NetApp SnapMirror.

> Lors de l'utilisation du chiffrement à la volée Kerberos avec les volumes NFSv4, vérifiez que les volumes NFSv4 utilisent les paramètres corrects. Reportez-vous à la section Configuration du domaine NetApp NFSv4 (page 13) du "Guide des améliorations et des bonnes pratiques de NetApp NFSv4".

Les données de sauvegarde restent dans le compartiment après leur suppression pour les compartiments dont la règle de conservation a expiré

Si vous supprimez la sauvegarde immuable d'une application après l'expiration de la politique de conservation du compartiment, la sauvegarde est supprimée d'Astra Control, mais pas du compartiment. Ce problème sera corrigé dans une prochaine version.

Trouvez plus d'informations

- "Limites connues"

Limites connues

Les limitations connues identifient les plateformes, les périphériques ou les fonctions qui ne sont pas pris en charge par cette version du produit, ou qui ne fonctionnent pas correctement avec elle. Examinez attentivement ces limites.

Limites de gestion du cluster

- Le même cluster ne peut pas être géré par deux instances Astra Control Center
- Astra Control Center ne peut pas gérer deux clusters nommés de manière identique

Limites du contrôle d'accès basé sur des rôles (RBAC)

- Un utilisateur doté de contraintes RBAC d'espace de noms peut ajouter et annuler la gestion d'un cluster
- Un membre avec des contraintes d'espace de noms ne peut pas accéder aux applications clonées ou restaurées tant que admin n'ajoute pas l'espace de noms à la contrainte

Limites de gestion des applications

- vous ne pouvez pas restaurer collectivement plusieurs applications dans un autre espace de noms
- ASTRA Control ne prend pas en charge les applications qui utilisent plusieurs classes de stockage par espace de noms
- Astra Control n'attribue pas automatiquement de compartiments par défaut pour les instances de cloud
- Les clones des applications installées à l'aide d'opérateurs pass-by-Reference peuvent échouer
- Les opérations de restauration sur place des applications qui utilisent un gestionnaire de certificats ne sont pas prises en charge
- Applications activées par OLM et déployées par l'opérateur à étendue de cluster non prises en charge
- Les applications déployées avec Helm 2 ne sont pas prises en charge
- Les snapshots peuvent échouer pour les clusters Kubernetes 1.25 ou versions ultérieures disposant de certaines versions de contrôleur Snapshot
- Il est possible que les sauvegardes et les snapshots ne soient pas conservés lors du retrait d'une instance Astra Control Center

Limitations générales

- Limitations de l'utilisateur et du groupe LDAP
- Les compartiments S3 du centre de contrôle Astra n'indiquent pas la capacité disponible
- Astra Control Center ne valide pas les détails que vous entrez pour votre serveur proxy
- Les connexions existantes à un pod Postgres provoquent des défaillances
- La page activité affiche jusqu'à 100000 événements
- SnapMirror ne prend pas en charge les applications utilisant NVMe over TCP pour les systèmes back-end de stockage

Le même cluster ne peut pas être géré par deux instances Astra Control Center

Si vous souhaitez gérer un cluster sur une autre instance Astra Control Center, vous devez d'abord "annuler la gestion du cluster" à partir de l'instance sur laquelle elle est gérée avant de la gérer sur une autre instance. Une fois le cluster supprimé de la gestion, vérifiez que le cluster n'est pas géré en exécutant la commande suivante :

```
oc get pods n -netapp-monitoring
```

Il ne doit y avoir aucun pod en cours d'exécution dans cet espace de nom, sinon l'espace de noms ne doit pas exister. Si l'un de ces deux éléments est vrai, le cluster n'est pas géré.

Astra Control Center ne peut pas gérer deux clusters nommés de manière identique

Si vous tentez d'ajouter un cluster portant le même nom qu'un cluster existant, l'opération échoue. Ce problème se produit le plus souvent dans un environnement Kubernetes standard si vous n'avez pas modifié le nom de cluster par défaut dans les fichiers de configuration Kubernetes.

Pour résoudre ce problème, procédez comme suit :

1. Modifiez votre `kubeadm-config` ConfigMap :

```
kubectl edit configmaps -n kube-system kubeadm-config
```

2. Modifiez le `clusterName` valeur de champ de `kubernetes` (Nom par défaut de Kubernetes) vers un nom personnalisé unique.
3. Modifiez kubecconfig (`.kube/config`).
4. Mettre à jour le nom de cluster depuis `kubernetes` à un nom personnalisé unique (`xyz-cluster` est utilisé dans les exemples ci-dessous). Effectuez la mise à jour dans les deux `clusters` et `contexts` sections comme indiqué dans cet exemple :

```
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data:
ExAmPLERb2tCcjZ5K3E2Njk4eQotLExAMpLEORCBDRVJUSUZJQ0FURS0txxxxXX==
    server: https://x.x.x.x:6443
  name: xyz-cluster
contexts:
- context:
    cluster: xyz-cluster
    namespace: default
    user: kubernetes-admin
  name: kubernetes-admin@kubernetes
current-context: kubernetes-admin@kubernetes
```

Un utilisateur doté de contraintes RBAC d'espace de noms peut ajouter et annuler la gestion d'un cluster

Un utilisateur doté de contraintes RBAC d'espace de noms ne doit pas être autorisé à ajouter ou annuler la gestion des clusters. En raison d'une limitation actuelle, Astra n'empêche pas ces utilisateurs de dégérer les clusters.

Un membre avec des contraintes d'espace de noms ne peut pas accéder aux applications clonées ou restaurées tant que admin n'ajoute pas l'espace de noms à la contrainte

Toutes `member` Les utilisateurs ayant des contraintes RBAC en fonction du nom/ID de l'espace de noms peuvent cloner ou restaurer une application vers un nouvel espace de noms sur le même cluster ou vers tout autre cluster du compte de leur entreprise. Cependant, le même utilisateur ne peut pas accéder à l'application clonée ou restaurée dans le nouvel espace de noms. Après la création d'un clone ou d'une opération de restauration, l'administrateur/propriétaire du compte peut modifier le `member` contraintes de compte d'utilisateur et de rôle de mise à jour pour l'utilisateur affecté pour accorder l'accès au nouvel espace de noms.

De même, vous ne pouvez pas restaurer collectivement plusieurs applications dans un autre espace de noms

Si vous gérez plusieurs applications dans un seul espace de noms (en créant plusieurs définitions d'applications dans Astra Control), vous ne pouvez pas restaurer toutes les applications dans un espace de noms différent. Chaque application doit être restaurée dans son propre espace de noms distinct.

ASTRA Control ne prend pas en charge les applications qui utilisent plusieurs classes de stockage par espace de noms

ASTRA Control prend en charge les applications qui utilisent une seule classe de stockage par espace de nom. Lorsque vous ajoutez une application à un espace de noms, assurez-vous que cette application possède la même classe de stockage que les autres applications de l'espace de noms.

Astra Control n'attribue pas automatiquement de compartiments par défaut pour les instances de cloud

Astra Control n'attribue pas automatiquement de compartiment par défaut à une instance de cloud. Vous devez définir manuellement un compartiment par défaut pour une instance de cloud. Si un compartiment par défaut n'est pas défini, vous ne pourrez pas effectuer les opérations de clonage d'applications entre les deux clusters.

Les clones des applications installées à l'aide d'opérateurs pass-by-Reference peuvent échouer

Astra Control prend en charge les applications installées avec des opérateurs à espace de noms. Ces opérateurs sont généralement conçus avec une architecture « pass-by-value » plutôt qu'une architecture « pass-by-Reference ». Voici quelques applications opérateur qui suivent ces modèles :

- "Apache K8ssandra"

> Pour K8ssandra, les opérations de restauration sur place sont prises en charge. Pour effectuer une opération de restauration vers un nouvel espace de noms ou un cluster, l'instance d'origine de l'application doit être arrêté. Cela permet de s'assurer que les informations du groupe de pairs transmises ne conduisent pas à une communication entre les instances. Le clonage de l'application n'est pas pris en charge.

- "IC Jenkins"
- "Cluster Percona XtraDB"

Astra Control peut ne pas être en mesure de cloner un opérateur conçu avec une architecture « pass-by-Reference » (par exemple, l'opérateur CockroachDB). Lors de ces types d'opérations de clonage, l'opérateur cloné tente de référencer les secrets de Kubernetes de l'opérateur source malgré avoir son propre nouveau secret dans le cadre du processus de clonage. Il est possible que le clonage échoue, car Astra Control ne connaît pas les secrets de Kubernetes qui sont présents dans l'opérateur source.

> Lors des opérations de clonage, les applications nécessitant une ressource IngressClass ou des crochets Web ne doivent pas avoir ces ressources déjà définies sur le cluster de destination.

Les opérations de restauration sur place des applications qui utilisent un gestionnaire de certificats ne sont pas prises en charge

Cette version d'Astra Control Center ne prend pas en charge la restauration sur place des applications avec des gestionnaires de certificats. Les opérations de restauration vers un espace de noms et des clones différents sont prises en charge.

Applications activées par OLM et déployées par l'opérateur à étendue de cluster non prises en charge

Astra Control Center ne prend pas en charge les activités de gestion d'applications avec des opérateurs à périmètre de cluster.

Les applications déployées avec Helm 2 ne sont pas prises en charge

Si vous utilisez Helm pour déployer des applications, Astra Control Center requiert Helm version 3. La gestion et le clonage des applications déployées avec Helm 3 (ou mises à niveau de Helm 2 à Helm 3) sont entièrement pris en charge. Pour plus d'informations, reportez-vous à la section "Exigences du centre de contrôle Astra".

Les snapshots peuvent échouer pour les clusters Kubernetes 1.25 ou versions ultérieures disposant de certaines versions de contrôleur Snapshot

Les snapshots pour les clusters Kubernetes exécutant la version 1.25 ou ultérieure peuvent échouer si la version v1beta1 des API du contrôleur de snapshot est installée sur le cluster.

Pour contourner ce problème, procédez comme suit lorsque vous mettez à niveau des installations Kubernetes 1.25 ou ultérieures :

1. Supprimez tous les CRD de snapshot existants et tout contrôleur de snapshot existant.
2. "Désinstaller Astra Trident".
3. "Installez les CRD de snapshot et le contrôleur de snapshot".
4. "Installez la dernière version d'Astra Trident".
5. "Créez une VolumeSnapshotClass".

Il est possible que les sauvegardes et les snapshots ne soient pas conservés lors du retrait d'une instance Astra Control Center

Si vous disposez d'une licence d'évaluation, veillez à stocker votre identifiant de compte afin d'éviter toute perte de données en cas d'échec du Centre de contrôle Astra si vous n'envoyez pas d'ASUP.

Limitations de l'utilisateur et du groupe LDAP

Astra Control Center prend en charge jusqu'à 5,000 groupes distants et 10,000 utilisateurs distants.

ASTRA Control ne prend pas en charge une entité LDAP (utilisateur ou groupe) qui a un DN contenant un RDN avec un espace de fin '\' ou un espace de fin.

Les compartiments S3 du centre de contrôle Astra n'indiquent pas la capacité disponible

Avant de sauvegarder ou de cloner des applications gérées par Astra Control Center, vérifiez les informations de compartiment dans le système de gestion ONTAP ou StorageGRID.

Astra Control Center ne valide pas les détails que vous entrez pour votre serveur proxy

Assurez-vous que vous "entrez les valeurs correctes" lors de l'établissement d'une connexion.

Les connexions existantes à un pod Postgres provoquent des défaillances

Lorsque vous exécutez des opérations sur les modules Postgres, vous ne devez pas vous connecter directement dans le pod pour utiliser la commande psql. Astra Control nécessite un accès psql pour geler et dégeler les bases de données. S'il existe une connexion existante, le snapshot, la sauvegarde ou le clone échoueront.

La page activité affiche jusqu'à 100000 événements

La page activité Astra Control peut afficher jusqu'à 100,000 événements. Pour afficher tous les événements consignés, récupérez-les à l'aide du "API de contrôle Astra".

SnapMirror ne prend pas en charge les applications utilisant NVMe over TCP pour les systèmes back-end de stockage

ASTRA Control Center ne prend pas en charge la réplication NetApp SnapMirror pour les systèmes back-end de stockage utilisant le protocole NVMe over TCP.

Trouvez plus d'informations

- "Problèmes connus"

Informations sur le copyright

Informations sur les marques commerciales