Notes de mise à jour

Astra Control Center

NetApp
November 21, 2023

This PDF was generated from https://docs.netapp.com/fr-fr/astra-control-center-2204/release-notes/whats-new.html on November 21, 2023. Always check docs.netapp.com for the latest.

Sommaire

Notes de mise à jour 1
Nouveautés de cette version d’Astra Control Center 1
Problèmes connus 2
Limites connues 4

Notes de mise à jour

Nous avons le plaisir d'annoncer la sortie 22.04.0 d'Astra Control Center.

- "Dans cette version d'Astra Control Center"
- "Problèmes connus"
- "Problèmes connus avec le magasin de données Astra et ce centre de contrôle Astra"
- "Limites connues"

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

Nouveautés de cette version d'Astra Control Center

Nous sommes heureux d'annoncer la dernière version 22.04.0 du Centre de contrôle Astra.

26 avril 2022 (22.04.0)

Nouvelles fonctionnalités et prises en charge

- "Déploiement d'un magasin de données Astra Control Center"
- "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"
- "Problèmes connus avec le magasin de données Astra et ce centre de contrôle Astra"
- "Restrictions connues pour cette version"

14 décembre 2021 (21.12)

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"
- "Découvrez la gestion et la surveillance du système back-end avec Astra Data Store"
- "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"
- "Problèmes connus avec la présentation d'Astra Data Store et ce centre de contrôle Astra"
- "Restrictions connues pour cette version"

5 août 2021 (21.08)

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"
- "Documentation Astra Data Store"
- "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 :

En applications

- La restauration d'une application entraîne une taille de volume persistant supérieure à celle de l'application initiale
- Les clones d'applications échouent à l'aide d'une version spécifique de PostgreSQL
- Les clones d'application échouent lors de l'utilisation des contraintes de contexte de sécurité OCP au niveau du compte de service (SCC)
- Les clones d'application échouent après le déploiement d'une application avec une classe de stockage définie

Clusters

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

Autres questions

- Les opérations de gestion des données d'application échouent avec l'erreur de service interne (500) lorsque Astra Trident est hors ligne
- Les snapshots peuvent échouer avec la version 4.2.0 du contrôleur de snapshot

La restauration d'une application entraîne une taille de volume persistant supérieure à celle de l'application initiale

Si vous redimensionnez un volume persistant après avoir créé une sauvegarde puis restauré à partir de cette sauvegarde, la taille du volume persistant correspond à la nouvelle taille du volume persistant, et non à la taille de la sauvegarde.

Les clones d'applications échouent à l'aide d'une version spécifique de PostgreSQL

Les clones d'applications au sein du même cluster échouent systématiquement avec le graphique Bitnami PostgreSQL 11.5.0. Pour effectuer un clonage réussi, utilisez une version antérieure ou ultérieure du graphique.

Les clones d'application échouent lors de l'utilisation des contraintes de contexte de sécurité OCP au niveau du compte de service (SCC)

Un clone d'application peut échouer si les contraintes de contexte de sécurité d'origine sont configurées au niveau du compte de service dans l'espace de noms du cluster OpenShift Container Platform. Lorsque le clone de l'application échoue, il apparaît dans la zone applications gérées du Centre de contrôle Astra avec l'état `Removed`. Voir la "article de la base de connaissances" pour en savoir plus.

Les clones d'application échouent après le déploiement d'une application avec une classe de stockage définie

Après le déploiement d'une application avec une classe de stockage définie explicitement (par exemple, `helm install …-set global.storageClass=netapp-cvs-perf-extreme`), les tentatives ultérieures de clonage de l'application nécessitent que le cluster cible ait la classe de stockage spécifiée à l'origine. Le clonage d'une application avec une classe de stockage définie explicitement dans un cluster ne disposant pas de la même classe de stockage échouera. Il n'y a pas d'étapes de récupération dans ce scénario.

La gestion d'un cluster avec Astra Control Center échoue lorsque le fichier kubeconfig par défaut 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.

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 snapshots peuvent échouer avec la version 4.2.0 du contrôleur de snapshot

Lorsque vous utilisez le snapshot-contrôleur Kubernetes (également appelé External-snapshotter) version

4.2.0 avec Kubernetes 1.20 ou 1.21, les snapshots peuvent échouer. Pour éviter cela, utilisez un autre "version prise en charge" D'un snapshoter externe, comme la version 4.2.1, avec Kubernetes version 1.20 ou 1.21.

1. Exécutez un appel POST pour ajouter un fichier kubeconfig mis à jour au `/credentials` et récupérer le noeud final affecté `id` du corps de réponse.
2. Effectuer un APPEL PUT à partir du `/clusters` À l'aide de l'ID de cluster approprié et définissez le `credentialID` à la `id` valeur de l'étape précédente.

Une fois ces étapes terminées, les informations d'identification associées au cluster sont mises à jour et le cluster doit se reconnecter et mettre à jour son état sur `available`.

Trouvez plus d'informations

- "Étude des problèmes connus avec le data Store d'Astra et ce centre de contrôle d'Astra"
- "Limites connues"

Problèmes connus avec le magasin de données Astra et ce centre de contrôle Astra

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

"Consultez ces problèmes connus" Il pourrait donc avoir un impact sur la gestion du magasin de données Astra avec la version actuelle du centre de contrôle Astra.

Trouvez plus d'informations

- "Problèmes connus"
- "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

- Les sauvegardes d'applications en cours ne peuvent pas être arrêtées
- 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

Limitations générales

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

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 carte de configuration kubeadm-config :

   ```
   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 ou des étiquettes 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 espace de noms par une opération de clonage ou de restauration, le compte admin/propriétaire 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.

Les sauvegardes d'applications en cours ne peuvent pas être arrêtées

Il est impossible d'arrêter une sauvegarde en cours d'exécution. Si vous devez supprimer la sauvegarde, attendez qu'elle soit terminée, puis suivez les instructions de la section "Supprimer les sauvegardes". Pour supprimer une sauvegarde ayant échoué, utilisez le "API de contrôle Astra".

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"

Notez qu'Astra Control peut ne pas être en mesure de cloner un opérateur conçu avec une architecture de "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.

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, voir "Exigences du centre de contrôle Astra".

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.

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.

Trouvez plus d'informations

- "Problèmes connus"
- "Problèmes connus avec le magasin de données Astra et ce centre de contrôle Astra"

Informations sur le copyright

Copyright © 2023 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.