Note di rilascio

Astra Control Center

NetApp
November 21, 2023

Sommario

Note di rilascio

Siamo lieti di annunciare l'ultima release di Astra Control Center.

- "Cosa c'è in questa release di Astra Control Center"
- "Problemi noti"
- "Limitazioni note"

Seguici su Twitter @NetAppDoc. Invia un feedback sulla documentazione diventando un "Collaboratore di GitHub" oppure inviare un'e-mail all'indirizzo doccomments@netapp.com.

Novità di questa release di Astra Control Center

Siamo lieti di annunciare l'ultima release di Astra Control Center.

22 novembre 2022 (22.11.0)

Nuove funzionalità e supporto

- "Supporto per applicazioni che si estendono su più spazi dei nomi"
- "Supporto per l'inclusione delle risorse cluster in una definizione applicativa"
- "Autenticazione LDAP avanzata con integrazione RBAC (role-based access control)"
- "Supporto aggiunto per Kubernetes 1.25 e Pod Security Admission (PSA)"
- "Report avanzati sui progressi delle operazioni di backup, ripristino e clonazione"

Problemi noti e limitazioni

- "Problemi noti per questa release"
- "Limitazioni note per questa versione"

8 settembre 2022 (22.08.1)

Questa release di patch (22.08.1) per Astra Control Center (22.08.0) corregge piccoli bug nella replica delle applicazioni utilizzando NetApp SnapMirror.

10 agosto 2022 (22.08.0)

Dettagli

Nuove funzionalità e supporto

- "Replica delle applicazioni con la tecnologia NetApp SnapMirror"
- "Miglioramento del workflow di gestione delle applicazioni"
- "Funzionalità migliorata di uncini di esecuzione personalizzati"

> I ganci di esecuzione predefiniti forniti da NetApp per le applicazioni specifiche sono stati rimossi in questa release. Se si esegue l'aggiornamento a questa release e non si forniscono i propri ganci di esecuzione per le snapshot, Astra Control eseguirà solo snapshot coerenti con il crash. Visitare il "Verda di NetApp" Repository GitHub per script hook di esecuzione di esempio che è possibile modificare per adattarsi al proprio ambiente.

- "Supporto per VMware Tanzu Kubernetes Grid Integrated Edition (TKGI)"
- "Supporto per Google anthos"
- "Configurazione LDAP (tramite Astra Control API)"

Problemi noti e limitazioni

- "Problemi noti per questa release"
- "Limitazioni note per questa versione"

26 aprile 2022 (22.04.0)

Dettagli

Nuove funzionalità e supporto

- "RBAC (role-based access control) dello spazio dei nomi"
- "Supporto per Cloud Volumes ONTAP"
- "Abilitazione ingresso generico per Astra Control Center"
- "Rimozione della benna da Astra Control"
- "Supporto per il portfolio VMware Tanzu"

Problemi noti e limitazioni

- "Problemi noti per questa release"
- "Limitazioni note per questa versione"

14 dicembre 2021 (21.12)

Dettagli

Nuove funzionalità e supporto

- "Ripristino dell'applicazione"
- "Ganci di esecuzione"
- "Supporto per le applicazioni implementate con operatori con ambito namespace"
- "Supporto aggiuntivo per Kubernetes e Rancher upstream"
- "Aggiornamenti di Astra Control Center"
- "Opzione Red Hat OperatorHub per l'installazione"

Problemi risolti

- "Problemi risolti per questa release"

Problemi noti e limitazioni

- "Problemi noti per questa release"
- "Limitazioni note per questa versione"

5 agosto 2021 (21.08)

Dettagli

Release iniziale di Astra Control Center.

- "Che cos'è"
- "Comprendere l'architettura e i componenti"
- "Cosa serve per iniziare"
- "Installare" e. "setup (configurazione)"
- "Gestire" e. "proteggere" applicazioni
- "Gestire i bucket" e. "back-end dello storage"
- "Gestire gli account"
- "Automatizzare con API"

Trova ulteriori informazioni

- "Problemi noti per questa release"
- "Limitazioni note per questa versione"
- "Versioni precedenti della documentazione di Astra Control Center"

Problemi noti

I problemi noti identificano i problemi che potrebbero impedire l'utilizzo corretto di questa versione del prodotto.

I seguenti problemi noti riguardano la versione corrente:

Applicazioni

- Il ripristino di un'applicazione comporta una dimensione PV superiore a quella del PV originale
- I cloni delle applicazioni non riescono a utilizzare una versione specifica di PostgreSQL
- I cloni delle applicazioni non funzionano quando si utilizzano i vincoli di contesto di protezione OCP a livello di account di servizio (SCC)
- I cloni delle applicazioni si guastano dopo l'implementazione di un'applicazione con una classe di storage set
- I backup e le snapshot delle applicazioni non vengono eseguiti se la classe volumesnapshotclass viene aggiunta dopo la gestione di un cluster

Cluster

- La gestione di un cluster con Astra Control Center non riesce quando il file kubeconfig predefinito contiene più di un contesto

Altri problemi

- I cluster gestiti non vengono visualizzati in NetApp Cloud Insights quando ci si connette tramite un proxy
- Le operazioni di gestione dei dati dell'app non riescono e si verificano errori di servizio interni (500) quando Astra Trident è offline

Il ripristino di un'applicazione comporta una dimensione PV superiore a quella del PV originale

Se si ridimensiona un volume persistente dopo la creazione di un backup e poi si ripristina da tale backup, le dimensioni del volume persistente corrispondono alle nuove dimensioni del PV invece di utilizzare le dimensioni del backup.

I cloni delle applicazioni non riescono a utilizzare una versione specifica di PostgreSQL

I cloni delle applicazioni all'interno dello stesso cluster si guastano costantemente con il grafico BitNami PostgreSQL 11.5.0. Per clonare correttamente, utilizzare una versione precedente o successiva del grafico.

I cloni delle applicazioni non funzionano quando si utilizzano i vincoli di contesto di protezione OCP a livello di account di servizio (SCC)

Un clone dell'applicazione potrebbe non riuscire se i vincoli del contesto di protezione originale sono configurati a livello di account di servizio all'interno dello spazio dei nomi nel cluster OpenShift Container Platform. Quando il clone dell'applicazione non funziona, viene visualizzato nell'area delle applicazioni gestite di Astra Control Center con lo stato `Removed`. Vedere "articolo della knowledge base" per ulteriori informazioni.

I backup e le snapshot delle applicazioni non vengono eseguiti se la classe volumesnapshotclass viene aggiunta dopo la gestione di un cluster

Backup e snapshot non vengono eseguiti con un `UI 500 error` in questo scenario. Come soluzione, aggiornare l'elenco delle applicazioni.

I cloni delle applicazioni si guastano dopo l'implementazione di un'applicazione con una classe di storage set

Dopo che un'applicazione è stata distribuita con una classe di storage esplicitamente impostata (ad esempio, `helm install …-set global.storageClass=netapp-cvs-perf-extreme`), i successivi tentativi di clonare l'applicazione richiedono che il cluster di destinazione abbia la classe di storage specificata in origine. La clonazione di un'applicazione con una classe di storage esplicitamente impostata su un cluster che non ha la stessa classe di storage non avrà esito positivo. In questo scenario non sono disponibili procedure di ripristino.

La gestione di un cluster con Astra Control Center non riesce quando il file kubeconfig predefinito contiene più di un contesto

Non è possibile utilizzare un kubeconfig con più di un cluster e un contesto. Vedere "articolo della knowledge base" per ulteriori informazioni.

I cluster gestiti non vengono visualizzati in NetApp Cloud Insights quando ci si connette tramite un proxy

Quando il centro di controllo Astra si connette a NetApp Cloud Insights tramite un proxy, i cluster gestiti potrebbero non essere visualizzati in Cloud Insights. Come soluzione alternativa, eseguire i seguenti comandi su ciascun cluster gestito:

```
kubectl get cm telegraf-conf -o yaml -n netapp-monitoring | sed
'/\[\[outputs.http\]\]/c\    [[outputs.http]]\n    use_system_proxy =
true' | kubectl replace -f -
```

```
kubectl get cm telegraf-conf-rs -o yaml -n netapp-monitoring | sed
'/\[\[outputs.http\]\]/c\    [[outputs.http]]\n    use_system_proxy =
true' | kubectl replace -f -
```

```
kubectl get pods -n netapp-monitoring --no-headers=true | grep 'telegraf-
ds\|telegraf-rs' | awk '{print $1}' | xargs kubectl delete -n netapp-
monitoring pod
```

Le operazioni di gestione dei dati dell'app non riescono e si verificano errori di servizio interni (500) quando Astra Trident è offline

Se Astra Trident su un cluster di applicazioni diventa offline (e viene riportato online) e si verificano 500 errori di servizio interni durante il tentativo di gestione dei dati dell'applicazione, riavviare tutti i nodi Kubernetes nel cluster di applicazioni per ripristinare la funzionalità.

Trova ulteriori informazioni

- "Limitazioni note"

Limitazioni note

Le limitazioni note identificano piattaforme, dispositivi o funzioni non supportate da questa versione del prodotto o che non interagiscono correttamente con esso. Esaminare attentamente queste limitazioni.

Limitazioni della gestione del cluster

- Lo stesso cluster non può essere gestito da due istanze di Astra Control Center
- Astra Control Center non è in grado di gestire due cluster con lo stesso nome

Limitazioni RBAC (Role-Based Access Control)

- Un utente con vincoli RBAC dello spazio dei nomi può aggiungere e annullare la gestione di un cluster
- Un membro con vincoli dello spazio dei nomi non può accedere alle applicazioni clonate o ripristinate fino a quando admin non aggiunge lo spazio dei nomi al vincolo

Limitazioni della gestione delle applicazioni

- Non è possibile ripristinare collettivamente più applicazioni in un singolo namespace in un namespace diverso
- Astra Control non assegna automaticamente i bucket predefiniti per le istanze cloud
- I cloni delle applicazioni installate utilizzando operatori pass-by-reference possono fallire
- Le operazioni di ripristino in-place delle applicazioni che utilizzano un gestore dei certificati non sono supportate
- Le applicazioni implementate dall'operatore CON ambito cluster e abilitato OLM non sono supportate
- Le app implementate con Helm 2 non sono supportate

Limitazioni generali

- I bucket S3 in Astra Control Center non riportano la capacità disponibile
- Astra Control Center non convalida i dati immessi per il server proxy
- Le connessioni esistenti a un pod Postgres causano errori
- I backup e le snapshot potrebbero non essere conservati durante la rimozione di un'istanza di Astra Control Center
- Limitazioni di utenti e gruppi LDAP

Lo stesso cluster non può essere gestito da due istanze di Astra Control Center

Se si desidera gestire un cluster su un'altra istanza di Astra Control Center, è necessario innanzitutto "annullare la gestione del cluster" dall'istanza in cui viene gestito prima di gestirlo su un'altra istanza. Dopo aver rimosso il cluster dalla gestione, verificare che il cluster non sia gestito eseguendo questo comando:

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

Non devono essere presenti pod in esecuzione nello spazio dei nomi, altrimenti lo spazio dei nomi non dovrebbe esistere. Se uno di questi è vero, il cluster non viene gestito.

Astra Control Center non è in grado di gestire due cluster con lo stesso nome

Se si tenta di aggiungere un cluster con lo stesso nome di un cluster già esistente, l'operazione non riesce. Questo problema si verifica più spesso in un ambiente Kubernetes standard se non è stato modificato il nome predefinito del cluster nei file di configurazione Kubernetes.

Per risolvere il problema, procedere come segue:

1. Modificare il `kubeadm-config` ConfigMap:

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

2. Modificare il `clusterName` valore campo da `kubernetes` (Il nome predefinito di Kubernetes) con un nome personalizzato univoco.
3. Modifica kubeconfig (`.kube/config`).
4. Aggiorna il nome del cluster da `kubernetes` su un nome personalizzato univoco (`xyz-cluster` viene utilizzato negli esempi seguenti). Eseguire l'aggiornamento in entrambi `clusters` e. `contexts` sezioni come mostrato in questo esempio:

```
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 utente con vincoli RBAC dello spazio dei nomi può aggiungere e annullare la gestione di un cluster

Un utente con vincoli RBAC dello spazio dei nomi non deve essere autorizzato ad aggiungere o annullare la gestione dei cluster. A causa di un limite corrente, Astra non impedisce a tali utenti di annullare la gestione dei cluster.

Un membro con vincoli dello spazio dei nomi non può accedere alle applicazioni clonate o ripristinate fino a quando admin non aggiunge lo spazio dei nomi al vincolo

Qualsiasi `member` Gli utenti con vincoli RBAC in base al nome/ID dello spazio dei nomi possono clonare o

ripristinare un'applicazione in un nuovo spazio dei nomi nello stesso cluster o in qualsiasi altro cluster nell'account dell'organizzazione. Tuttavia, lo stesso utente non può accedere all'applicazione clonata o ripristinata nel nuovo namespace. Una volta creato un nuovo spazio dei nomi mediante un'operazione di clonazione o ripristino, l'amministratore/proprietario dell'account può modificare `member` account utente e limitazioni del ruolo di aggiornamento per consentire all'utente interessato di concedere l'accesso al nuovo spazio dei nomi.

Non è possibile ripristinare collettivamente più applicazioni in un singolo namespace in un namespace diverso

Se si gestiscono più applicazioni in un singolo namespace (creando più definizioni di applicazioni in Astra Control), non è possibile ripristinare tutte le applicazioni in un singolo namespace diverso. È necessario ripristinare ogni applicazione nel proprio spazio dei nomi separato.

Astra Control non assegna automaticamente i bucket predefiniti per le istanze cloud

Astra Control non assegna automaticamente un bucket predefinito per nessuna istanza di cloud. È necessario impostare manualmente un bucket predefinito per un'istanza di cloud. Se non viene impostato un bucket predefinito, non sarà possibile eseguire operazioni di cloni tra due cluster.

I cloni delle applicazioni installate utilizzando operatori pass-by-reference possono fallire

Astra Control supporta le applicazioni installate con operatori con ambito namespace. Questi operatori sono generalmente progettati con un'architettura "pass-by-value" piuttosto che "pass-by-reference". Di seguito sono riportate alcune applicazioni per operatori che seguono questi modelli:

- "Apache K8ssandra"

> Per K8ssandra, sono supportate le operazioni di ripristino in-place. Un'operazione di ripristino su un nuovo namespace o cluster richiede che l'istanza originale dell'applicazione venga tolto. In questo modo si garantisce che le informazioni del peer group trasportate non conducano a comunicazioni tra istanze. La clonazione dell'applicazione non è supportata.

- "Ci Jenkins"
- "Cluster XtraDB Percona"

Astra Control potrebbe non essere in grado di clonare un operatore progettato con un'architettura "pass-by-reference" (ad esempio, l'operatore CockroachDB). Durante questi tipi di operazioni di cloning, l'operatore clonato tenta di fare riferimento ai segreti di Kubernetes dall'operatore di origine, nonostante abbia il proprio nuovo segreto come parte del processo di cloning. L'operazione di clonazione potrebbe non riuscire perché Astra Control non è a conoscenza dei segreti di Kubernetes nell'operatore di origine.

> Durante le operazioni di cloni, le applicazioni che necessitano di una risorsa IngressClass o di webhook per funzionare correttamente non devono disporre di tali risorse già definite nel cluster di destinazione.

Le operazioni di ripristino in-place delle applicazioni che utilizzano un gestore dei certificati non sono supportate

Questa versione di Astra Control Center non supporta il ripristino in-place delle applicazioni con i gestori dei certificati. Sono supportate le operazioni di ripristino su uno spazio dei nomi diverso e le operazioni di clonazione.

Le applicazioni implementate dall'operatore CON ambito cluster e abilitato OLM non sono supportate

Astra Control Center non supporta le attività di gestione delle applicazioni con operatori con ambito cluster.

Le app implementate con Helm 2 non sono supportate

Se utilizzi Helm per implementare le app, Astra Control Center richiede Helm versione 3. La gestione e la clonazione delle applicazioni implementate con Helm 3 (o aggiornate da Helm 2 a Helm 3) sono completamente supportate. Per ulteriori informazioni, vedere "Requisiti di Astra Control Center".

I bucket S3 in Astra Control Center non riportano la capacità disponibile

Prima di eseguire il backup o la clonazione delle applicazioni gestite da Astra Control Center, controllare le informazioni del bucket nel sistema di gestione ONTAP o StorageGRID.

Astra Control Center non convalida i dati immessi per il server proxy

Assicurati di "inserire i valori corretti" quando si stabilisce una connessione.

Le connessioni esistenti a un pod Postgres causano errori

Quando si eseguono operazioni su POD Postgres, non si dovrebbe connettersi direttamente all'interno del pod per utilizzare il comando psql. Astra Control richiede l'accesso a psql per bloccare e scongelare i database. Se è presente una connessione preesistente, lo snapshot, il backup o il clone non avranno esito positivo.

I backup e le snapshot potrebbero non essere conservati durante la rimozione di un'istanza di Astra Control Center

Se si dispone di una licenza di valutazione, assicurarsi di memorizzare l'ID account per evitare la perdita di dati in caso di guasto di Astra Control Center se non si inviano ASUP.

Limitazioni di utenti e gruppi LDAP

Astra Control Center supporta fino a 5,000 gruppi remoti e 10,000 utenti remoti.

Trova ulteriori informazioni

- "Problemi noti"

Informazioni sul copyright

Informazioni sul marchio commerciale