Note di rilascio

Astra Control Center

NetApp
June 06, 2024

Sommario

Note di rilascio

Siamo lieti di annunciare la release iniziale 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.

Cosa c'è in questa release di Astra Control Center

Siamo lieti di annunciare il rilascio di Astra Control Center.

5 agosto 2021 (21.08)

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"

Problemi noti relativi a questa versione

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:

- ClusterRoleBinding non corretto creato da Astra Control Center CRD durante l'installazione
- L'applicazione con etichetta definita dall'utente passa allo stato "removed" (rimosso)
- Impossibile interrompere l'esecuzione del backup dell'applicazione
- Il backup o il clone non riesce per le applicazioni che utilizzano PVC con unità decimali in Astra Control Center
- ad esempio le modifiche persistenti del volume

- Trident crea un PV più grande del PV originale
- Clonare le performance influenzate da grandi volumi persistenti
- 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 bucket S3 in Astra Control Center non riportano la capacità disponibile
- Il riutilizzo dei bucket tra istanze di Astra Control Center causa errori
- La selezione di un tipo di provider bucket con credenziali per un altro tipo causa errori di protezione dei dati
- I backup e le snapshot potrebbero non essere conservati durante la rimozione di un'istanza di Astra Control Center
- I backup aggiuntivi vengono conservati come parte del backup pianificato
- "L'operazione di cloning non può utilizzare altri bucket oltre a quelli predefiniti"
- La gestione di un cluster con Astra Control Center non riesce quando il file kubeconfig predefinito contiene più di un contesto
- "Impossibile determinare lo stato del bundle tar ASUP in un ambiente scalato"
- La disinstallazione di Astra Control Center non riesce a pulire il pod operatore di monitoraggio sul cluster gestito
- La disinstallazione di Astra Control Center non consente di eliminare i CRD Traefik
- Raccolta ASUP bloccata in uno stato di generazione o caricamento

ClusterRoleBinding non corretto creato da Astra Control Center CRD durante l'installazione

Applicare la seguente patch a tutti i cluster Kubernetes in cui è stata implementata la versione 21.08.65 dell'operatore acc. Deve essere applicato anche se l'operatore acc viene riattivato.

Per risolvere questo problema:

1. Sostituire `ACC_NAMESPACE` nello script riportato di seguito con lo spazio dei nomi utilizzato "Implementare Astra Control Center".

```
cat <<EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: acc-operator-manager-rolebinding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: acc-operator-manager-role
subjects:
- kind: ServiceAccount
  name: default
  namespace: netapp-acc-operator
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: system:serviceaccounts:ACC_NAMESPACE
EOF
```

2. Eseguire lo script.

Il cerotto rimuove i seguenti due soggetti `ClusterRoleBinding: "acc-operator-manager-rolebinding"`

```
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: system:serviceaccounts
- apiGroup: ""
  kind: Group
  name: system:serviceaccounts
```

L'applicazione con etichetta definita dall'utente passa allo stato "removed" (rimosso)

Se definisci un'applicazione con un'etichetta k8s inesistente, Astra Control Center creerà, gestirà e rimuoverà immediatamente l'applicazione. Per evitare questo problema, Aggiungi l'etichetta k8s ai pod e alle risorse dopo che l'applicazione è stata gestita da Astra Control Center.

Impossibile interrompere l'esecuzione del backup dell'applicazione

Non esiste alcun modo per interrompere un backup in esecuzione. Se è necessario eliminare il backup, attendere che sia stato completato, quindi seguire le istruzioni riportate in "Eliminare i backup". Per eliminare un backup non riuscito, utilizzare "API Astra".

Il backup o il clone non riesce per le applicazioni che utilizzano PVC con unità decimali in Astra Control Center

I volumi creati con unità decimali non riescono utilizzando il processo di backup o clone di Astra Control Center. Vedere "articolo della knowledge base" per ulteriori informazioni.

L'interfaccia utente di Astra Control Center mostra lentamente le modifiche apportate alle risorse dell'applicazione, ad esempio le modifiche persistenti del volume

Dopo un'operazione di protezione dei dati (clone, backup, ripristino) e il successivo ridimensionamento persistente del volume, si verifica un ritardo di venti minuti prima che le nuove dimensioni del volume vengano visualizzate nell'interfaccia utente. Questo ritardo nell'interfaccia utente può verificarsi anche quando vengono aggiunte o modificate le risorse dell'applicazione. In questo caso, un'operazione di protezione dei dati viene eseguita correttamente in pochi minuti ed è possibile utilizzare il software di gestione per il back-end dello storage per confermare la modifica delle dimensioni del volume.

Durante il ripristino dell'applicazione dal backup, Trident crea un PV più grande 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.

Clonare le performance influenzate da grandi volumi persistenti

I cloni di volumi persistenti molto grandi e consumati potrebbero essere lenti a intermittenza, a seconda dell'accesso del cluster all'archivio di oggetti. Se il clone viene bloccato e non sono stati copiati dati per più di 30 minuti, Astra Control termina l'azione del clone.

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 OCP. 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 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.

Il riutilizzo dei bucket tra istanze di Astra Control Center causa errori

Se si tenta di riutilizzare un bucket utilizzato da un'altra o da un'altra installazione di Astra Control Center, il

backup e il ripristino non avranno esito positivo. È necessario utilizzare una benna diversa o pulire completamente la benna utilizzata in precedenza. Non è possibile condividere i bucket tra istanze di Astra Control Center.

La selezione di un tipo di provider bucket con credenziali per un altro tipo causa errori di protezione dei dati

Quando si aggiunge un bucket, selezionare il tipo di provider bucket corretto con le credenziali corrette per tale provider. Ad esempio, l'interfaccia utente accetta NetApp ONTAP S3 come tipo con credenziali StorageGRID; tuttavia, questo causerà l'errore di tutti i backup e ripristini futuri dell'applicazione che utilizzano questo bucket.

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.

I backup aggiuntivi vengono conservati come parte del backup pianificato

A volte uno o più backup in Astra Control Center vengono conservati oltre il numero specificato per essere conservati nella pianificazione del backup. Questi backup aggiuntivi devono essere cancellati come parte di un backup pianificato, ma non vengono cancellati e bloccati in un `pending` stato. Per risolvere il problema, "forza eliminazione" i backup aggiuntivi.

L'operazione di cloning non può utilizzare altri bucket oltre a quelli predefiniti

Durante il backup di un'applicazione o il ripristino di un'applicazione, è possibile specificare un ID bucket. Un'operazione di cloni dell'applicazione, tuttavia, utilizza sempre il bucket predefinito definito. Non esiste alcuna opzione per modificare i bucket per un clone. Se si desidera controllare quale bucket viene utilizzato, è possibile farlo "modificare l'impostazione predefinita del bucket" oppure fare una "backup" seguito da un "ripristinare" separatamente.

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.

Impossibile determinare lo stato del bundle tar ASUP in un ambiente scalato

Durante la raccolta ASUP, lo stato del bundle nell'interfaccia utente viene riportato come uno dei due `collecting` oppure `done`. La raccolta può richiedere fino a un'ora per ambienti di grandi dimensioni. Durante il download di ASUP, la velocità di trasferimento dei file di rete per il bundle potrebbe essere insufficiente e il download potrebbe scadere dopo 15 minuti senza alcuna indicazione nell'interfaccia utente. I problemi di download dipendono dalle dimensioni dell'ASUP, dalle dimensioni del cluster scalate e se il tempo di raccolta supera il limite di sette giorni.

La disinstallazione di Astra Control Center non riesce a pulire il pod operatore di monitoraggio sul cluster gestito

Se i cluster non sono stati disgestiti prima della disinstallazione di Astra Control Center, è possibile eliminare manualmente i pod nello spazio dei nomi di monitoraggio netapp e nello spazio dei nomi con i seguenti

comandi:

Fasi

1. Eliminare `acc-monitoring` agente:

```
oc delete agents acc-monitoring -n netapp-monitoring
```

Risultato:

```
agent.monitoring.netapp.com "acc-monitoring" deleted
```

2. Eliminare lo spazio dei nomi:

```
oc delete ns netapp-monitoring
```

Risultato:

```
namespace "netapp-monitoring" deleted
```

3. Conferma la rimozione delle risorse:

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

Risultato:

```
No resources found in netapp-monitoring namespace.
```

4. Conferma rimozione dell'agente di monitoraggio:

```
oc get crd|grep agent
```

Risultato del campione:

```
agents.monitoring.netapp.com                    2021-07-21T06:08:13Z
```

5. Eliminare le informazioni CRD (Custom Resource Definition):

```
oc delete crds agents.monitoring.netapp.com
```

Risultato:

```
customresourcedefinition.apiextensions.k8s.io
"agents.monitoring.netapp.com" deleted
```

La disinstallazione di Astra Control Center non consente di eliminare i CRD Traefik

È possibile eliminare manualmente i CRD Traefik:

Fasi

1. Verificare quali CRD non sono stati eliminati dal processo di disinstallazione:

```
kubectl get crds |grep -E 'traefik'
```

Risposta

```
ingressroutes.traefik.containo.us             2021-06-23T23:29:11Z
ingressroutetcps.traefik.containo.us          2021-06-23T23:29:11Z
ingressrouteudps.traefik.containo.us          2021-06-23T23:29:12Z
middlewares.traefik.containo.us               2021-06-23T23:29:12Z
serverstransports.traefik.containo.us         2021-06-23T23:29:13Z
tlsoptions.traefik.containo.us                2021-06-23T23:29:13Z
tlsstores.traefik.containo.us                 2021-06-23T23:29:14Z
traefikservices.traefik.containo.us           2021-06-23T23:29:15Z
```

2. Eliminare i CRD:

```
kubectl delete crd ingressroutes.traefik.containo.us
ingressroutetcps.traefik.containo.us
ingressrouteudps.traefik.containo.us middlewares.traefik.containo.us
serverstransports.traefik.containo.us tlsoptions.traefik.containo.us
tlsstores.traefik.containo.us traefikservices.traefik.containo.us
```

Raccolta ASUP bloccata in uno stato di generazione o caricamento

Se un pod ASUP viene ucciso o riavviato, una raccolta ASUP potrebbe bloccarsi in uno stato di generazione o caricamento. Effettuare le seguenti operazioni "API REST di Astra Control" chiamata per avviare nuovamente la raccolta manuale:

Metodo HTTP	Percorso
POST	/Accounts/{AccountID}/core/v1/asups

Questa soluzione alternativa API funziona solo se eseguita più di 10 minuti dopo l'avvio di ASUP.

Trova ulteriori informazioni

- "Limitazioni note per questa versione"

Limitazioni note di questa versione

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.

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.

Il cluster è in `removed` stato anche se il cluster e la rete funzionano in modo diverso come previsto

Se un cluster si trova in `removed` state Yet la connettività di rete e del cluster sembra sana (i tentativi esterni di accesso al cluster utilizzando le API di Kubernetes sono riusciti), il kubeconfig che hai fornito ad Astra Control potrebbe non essere più valido. Ciò può essere dovuto alla rotazione o alla scadenza del certificato sul cluster. Per risolvere questo problema, aggiornare le credenziali associate al cluster in Astra Control utilizzando "API di controllo Astra":

1. Eseguire UNA CHIAMATA POST per aggiungere un file kubeconfig aggiornato a `/credentials` endpoint e recuperare l'assegnato `id` dal corpo di risposta.
2. Eseguire una chiamata PUT da `/clusters` Endpoint utilizzando l'ID cluster appropriato e impostare `credentialID` al `id` valore dal passo precedente.

Una volta completata questa procedura, la credenziale associata al cluster viene aggiornata e il cluster si riconnetterà e aggiornerà il proprio stato a. `available`.

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

Astra Control Center non supporta le applicazioni implementate con operatori abilitati per Operator Lifecycle Manager (OLM) o con gli operatori con ambito cluster.

La clonazione delle applicazioni può essere eseguita solo con la stessa distribuzione K8s

Se clonate un'applicazione tra cluster, i cluster di origine e di destinazione devono essere la stessa distribuzione di Kubernetes. Ad esempio, se clonate un'applicazione da un cluster OpenShift 4.7, utilizzate un cluster di destinazione che è anche OpenShift 4.7.

OpenShift 4.8 non è supportato

OpenShift 4.8 non è supportato per la release di luglio di Astra Control Center. Per ulteriori informazioni, vedere "Requisiti di Astra Control Center".

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".

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

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

Data Protection per Astra Control Center come applicazione non ancora disponibile

Questa release non supporta la possibilità di gestire Astra come applicazione utilizzando opzioni di snapshot, backup o ripristino.

I pod non integri influiscono sulla gestione delle applicazioni

Se un'applicazione gestita ha dei pod in uno stato non integro, Astra Control non può creare nuovi backup e cloni.

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.

Trident non viene disinstallato da un cluster

Quando si disgestisce un cluster da Astra Control Center, Trident non viene disinstallato automaticamente dal cluster. Per disinstallare Trident, è necessario "Seguire questa procedura nella documentazione di Trident".

Trova ulteriori informazioni

- "Problemi noti per questa release"

Informazioni sul copyright

Informazioni sul marchio commerciale