



## **Note di rilascio**

### **Astra Control Center**

NetApp  
November 21, 2023

This PDF was generated from <https://docs.netapp.com/it-it/astra-control-center-2112/release-notes/whats-new.html> on November 21, 2023. Always check docs.netapp.com for the latest.

# Sommario

- Note di rilascio ..... 1
  - Novità di questa release di Astra Control Center ..... 1
  - Problemi risolti ..... 2
  - Problemi noti con l’anteprima di Astra Data Store e questa release di Astra Control Center ..... 3
  - Problemi noti ..... 5
  - Limitazioni note ..... 11

# Note di rilascio

Siamo lieti di annunciare la release 21.12 di Astra Control Center.

- ["Cosa c'è in questa release di Astra Control Center"](#)
- ["Problemi risolti"](#)
- ["Problemi noti"](#)
- ["Problemi noti con l'anteprima di Astra Data Store e questa release di Astra Control Center"](#)
- ["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](mailto:doccomments@netapp.com).

## Novità di questa release di Astra Control Center

Siamo lieti di annunciare l'ultima release 21.12 di Astra Control Center.

### 14 dicembre 2021 (21.12)

Release aggiornata di Astra Control Center.

#### 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"](#)
- ["Astra Data Store visualizza in anteprima la gestione e il monitoraggio del back-end"](#)
- ["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"](#)
- ["Problemi noti con l'anteprima di Astra Data Store e questa release di Astra Control Center"](#)
- ["Limitazioni note per questa versione"](#)

### 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"](#)
- ["Documentazione di Astra Data Store"](#)
- ["Versioni precedenti della documentazione di Astra Control Center"](#)

## Problemi risolti

Questi problemi sono stati corretti in questa versione del prodotto.

### **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.

### **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.

### **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.

### **Associazione errata del ruolo del cluster creata dalla definizione di risorsa personalizzata di Astra Control Center durante l'installazione**

La patch per correggere l'associazione del ruolo del cluster durante l'installazione non è più necessaria in questa release.

## Raccolta ASUP bloccata in uno stato di generazione o caricamento

Se un pod ASUP viene arrestato o riavviato, una raccolta ASUP potrebbe bloccarsi in uno stato di generazione o caricamento.

## Applicazioni e spazi dei nomi implementati dall'operatore

Un operatore e l'applicazione che implementa devono utilizzare lo stesso namespace. Astra Control supporta solo un'applicazione implementata dall'operatore per spazio dei nomi.

## Trova ulteriori informazioni

- ["Problemi noti"](#)
- ["Limitazioni note"](#)
- ["Problemi noti con l'anteprima di Astra Data Store e questa release di Astra Control Center"](#)

## Problemi noti con l'anteprima di Astra Data Store e questa release di Astra Control Center

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

I seguenti problemi noti influiscono sulla gestione di Astra Data Store con questa versione corrente di Astra Control Center:

### L'anteprima di Astra Data Store non può essere utilizzata come classe di storage per Astra Control Center a causa di un guasto alla sonda di liveness del pod MongoDB

Quando si tenta di utilizzare l'anteprima di Astra Data Store come provider di classi di storage durante un'implementazione di Astra Control Center, la sonda di liveness del pod MongoDB non funziona, con un risultato che non verrà completato.

Per correggere questo problema, apportare le seguenti modifiche oltre alle modifiche YAML standard al completamento di ["Processo di installazione di Astra Control Center"](#):

1. Modificare il ["Implementazione YAML dell'operatore di Astra Control Center \(astra\\_control\\_center\\_operator\\_deploy.yaml\)"](#) Per modificare il timeout di installazione Helm:

```
- name: ACCOP_HELM_INSTALLTIMEOUT
  value: 20m
```

2. Modificare il ["File di risorse personalizzate \(CR\) di Astra Control Center \(astra\\_control\\_center\\_min.yaml\)"](#) e includere i valori aggiuntivi evidenziati in `spec`:

```

apiVersion: astra.netapp.io/v1
kind: AstraControlCenter
metadata:
  name: astra
spec:
  accountName: "Example"
  astraVersion: "ASTRA_VERSION"
  astraAddress: "astra.example.com"
  autoSupport:
    enrolled: true
  email: "[admin@example.com]"
  firstName: "SRE"
  lastName: "Admin"
  imageRegistry:
    name: "[your_registry_path]"
    secret: "astra-registry-cred"
  storageClass: "ontap-gold"
  additionalValues:
    polaris-mongodb:
      mongodb:
        livenessProbe:
          initialDelaySeconds: 400
      metrics:
        livenessProbe:
          initialDelaySeconds: 400

```

## Astra Control Center mostra il backend dello storage di anteprima di Astra Data Store Unknown stato

Astra Control Center mostra il backend dello storage di anteprima Astra Data Store in un Unknown dalla pagina backend nell'interfaccia utente. In questa condizione, il backend dello storage è effettivamente disponibile e può essere comunicato con. Un componente all'interno del back-end dello storage è probabilmente in uno stato non integro e deve essere riportato a uno stato integro affinché il back-end dello storage venga visualizzato come available.

### Trova ulteriori informazioni

- ["Problemi risolti"](#)
- ["Problemi noti"](#)
- ["Limitazioni note"](#)
- ["Documentazione di Astra Data Store"](#)

# 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:

- L'applicazione con etichetta definita dall'utente passa allo stato "removed" (rimosso)
- Impossibile interrompere l'esecuzione del backup dell'applicazione
- 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)
- 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
- "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
- 500 errore di servizio interno durante il tentativo di gestione dei dati dell'applicazione Trident
- Gli script hook di esecuzione delle applicazioni personalizzate non vengono eseguiti e gli script post-snapshot non vengono eseguiti
- "Impossibile determinare lo stato del bundle tar ASUP in un ambiente scalato"
- Le snapshot iniziano a fallire quando si utilizza la versione 4.2.0 di external-snapshotter
- Le operazioni di ripristino simultanee delle applicazioni nello stesso namespace possono avere esito negativo
- L'aggiornamento non riesce se la versione di origine utilizza un Registro di sistema di immagine container che non richiede autenticazione e la versione di destinazione utilizza un Registro di sistema di immagine container che richiede autenticazione
- 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

## 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 di controllo Astra"](#).

## **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 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.

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

Se si tenta di riutilizzare un bucket utilizzato da un'altra installazione o da una precedente installazione di Astra Control Center, le operazioni di backup e 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 bucket provider corretto e immettere le credenziali corrette per tale provider. Ad esempio, l'interfaccia utente accetta come tipo NetApp ONTAP S3 e accetta le 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.

## **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.

## **500 errore di servizio interno durante il tentativo di gestione dei dati dell'applicazione Trident**

Se Trident su un cluster di applicazioni diventa offline (e viene riportato online) e si verificano errori di servizio interni 500 quando si tenta di gestire i dati delle applicazioni, riavviare tutti i nodi Kubernetes nel cluster di applicazioni per ripristinare la funzionalità.

## **Gli script hook di esecuzione delle applicazioni personalizzate non vengono eseguiti e gli script post-snapshot non vengono eseguiti**

Se l'esecuzione di un gancio di esecuzione richiede più di 25 minuti, l'hook non riesce, creando una voce del registro eventi con un codice di ritorno "N/A". Qualsiasi snapshot interessata verrà contrassegnata come non riuscita e una voce del registro eventi risultante ne annoterà il timeout.

Poiché gli hook di esecuzione spesso riducono o disattivano completamente le funzionalità dell'applicazione con cui vengono eseguiti, si consiglia di ridurre al minimo il tempo necessario per l'esecuzione degli hook di esecuzione personalizzati.

## **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 scalato e se il tempo di raccolta supera il limite di sette giorni.

## Le snapshot iniziano a fallire quando si utilizza la versione 4.2.0 di external-snapshotter

Quando si utilizza Kubernetes snapshot-controller (noto anche come external-snapshotter) versione 4.2.0 con Kubernetes 1.20 o 1.21, le snapshot possono iniziare a fallire. Per evitare questo problema, utilizzare un altro "versione supportata" Di external-snapshotter, come la versione 4.2.1, con Kubernetes versioni 1.20 o 1.21.

## Le operazioni di ripristino simultanee delle applicazioni nello stesso namespace possono avere esito negativo

Se si tenta di ripristinare contemporaneamente una o più applicazioni gestite singolarmente all'interno di uno spazio dei nomi, le operazioni di ripristino possono fallire dopo un lungo periodo di tempo. Come soluzione alternativa, ripristinare ciascuna applicazione una alla volta.

## L'aggiornamento non riesce se la versione di origine utilizza un Registro di sistema di immagine container che non richiede autenticazione e la versione di destinazione utilizza un Registro di sistema di immagine container che richiede autenticazione

Se si aggiorna un sistema Astra Control Center che utilizza un registro che non richiede l'autenticazione a una versione più recente che utilizza un registro che richiede l'autenticazione, l'aggiornamento non riesce. Per risolvere il problema, attenersi alla seguente procedura:

1. Accedere a un host con accesso di rete al cluster Astra Control Center.
2. Assicurarsi che l'host disponga della seguente configurazione:
  - kubectl è installata la versione 1.19 o successiva
  - La variabile di ambiente KUBECONFIG viene impostata sul file kubeconfig per il cluster Astra Control Center
3. Eseguire il seguente script:

```
namespace="<netapp-acc>"
statefulsets=("polaris-vault" "polaris-mongodb" "influxdb2" "nats"
"loki")
for ss in ${statefulsets[@]}; do
    existing=$(kubectl get -n ${namespace} statefulsets.apps ${ss} -o
jsonpath='{.spec.template.spec.imagePullSecrets}')
    if [ "${existing}" = "[]" ] || [ "${existing}" = "[{} , {} , {}]" ];
then
        kubectl patch -n ${namespace} statefulsets.apps ${ss} --type
merge --patch '{"spec": {"template": {"spec": {"imagePullSecrets":
[]}}}}'
    else
        echo "${ss} not patched"
    fi
done
```

L'output dovrebbe essere simile a quanto segue:

```
statefulset.apps/polaris-vault patched
statefulset.apps/polaris-mongodb patched
statefulset.apps/influxdb2 patched
statefulset.apps/nats patched
statefulset.apps/loki patched
```

4. Procedere con l'aggiornamento utilizzando ["Istruzioni per l'aggiornamento di Astra Control Center"](#).

## 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. Le CRDS sono risorse globali e l'eliminazione di queste risorse potrebbe avere un impatto sulle altre applicazioni del cluster.

### Fasi

#### 1. Elencare i CRD Traefik installati sul cluster:

```
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  
middlewareetcps.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
middlewareetcps.traefik.containo.us
```

## Trova ulteriori informazioni

- ["Problemi risolti"](#)
- ["Problemi noti con la prreview di Astra Data Store e questa release di Astra Control Center"](#)
- ["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.

### 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 nello stesso cloud

Se si tenta di aggiungere un cluster con lo stesso nome di un cluster già esistente nel cloud, 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. Modifica la configurazione di kubeadm-config:

```
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
```

## I cloni delle applicazioni installate utilizzando gli operatori di riferimento pass-by 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"](#)
- ["Ci Jenkins"](#)
- ["Cluster XtraDB Percona"](#)

Si noti che 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.

## 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.

## **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.

## **MetalLB 0.11.0 non è supportato**

MetalLB 0.11.0 non è un bilanciamento del carico supportato per Astra Control Center. Per ulteriori informazioni sui bilanciatori di carico supportati, 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 risolti"](#)
- ["Problemi noti"](#)
- ["Problemi noti con l'anteprima di Astra Data Store e questa release di Astra Control Center"](#)



## Informazioni sul copyright

Copyright © 2023 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.