



## **Note di rilascio**

### **Astra Control Service**

NetApp  
June 04, 2024

# Sommario

- Note di rilascio ..... 1
- Novità di Astra Control Service ..... 1
- Problemi noti ..... 10
- Limitazioni note ..... 12

# Note di rilascio

## Novità di Astra Control Service

NetApp aggiorna periodicamente Astra Control Service per offrire nuove funzionalità, miglioramenti e correzioni di bug.

### 14 marzo 2024

#### (Anteprima tecnica) flussi di lavoro Kubernetes dichiarativi

Questa release di Astra Control Service contiene una funzionalità dichiarativa di Kubernetes che consente di eseguire la gestione dei dati da una risorsa personalizzata (CR) di Kubernetes nativa.

Questa funzionalità è disponibile solo nell'istanza del programma EAP (Early Adopter Program) del servizio Astra Control. Per informazioni sulla partecipazione al programma EAP, contattare il rappresentante commerciale NetApp di zona.

Dopo l'installazione di "[Connettore Astra](#)" Nel cluster che si desidera gestire, è possibile eseguire le seguenti operazioni cluster basate su CR nell'interfaccia utente o da una CR:

- ["Definire un'applicazione utilizzando una risorsa personalizzata"](#)
- ["Definire il bucket"](#)
- ["Protezione di un intero cluster"](#)
- ["Eseguire il backup dell'applicazione"](#)
- ["Creare un'istantanea"](#)
- ["Creare pianificazioni per snapshot o backup"](#)
- ["Ripristinare un'applicazione da uno snapshot o da un backup"](#)

### 7 novembre 2023

#### Nuove funzionalità e supporto

- **Funzionalità di backup e ripristino per applicazioni con backend di storage ontap-nas-Economy con driver-backend:** Abilita le operazioni di backup e ripristino per `ontap-nas-economy` con alcuni ["semplici passaggi"](#).
- **Supporto di Astra Control Service per i cluster Red Hat OpenShift Container Platform on-premise**  
["Aggiungere un cluster"](#)
- **Backup immutabili:** Astra Control ora supporta ["backup di sola lettura inalterabili"](#) come livello di sicurezza aggiuntivo contro malware e altre minacce.
- **Presentazione di Astra Control Provisioner**

Con la release 23,10, Astra Control introduce un nuovo componente software chiamato Astra Control Provisioner, che sarà disponibile per tutti gli utenti di Astra Control con licenza. Astra Control Provisioner offre l'accesso a un superset di funzionalità avanzate di gestione e provisioning dello storage oltre a quelle offerte da Astra Trident. Queste funzionalità sono disponibili per tutti i clienti Astra Control senza costi aggiuntivi.

- **Inizia con Astra Control Provisioner**

È possibile ["Abilita Astra Control Provisioner"](#) Se hai installato e configurato il tuo ambiente per l'utilizzo di Astra Trident 23,10.

- **Funzionalità di Astra Control Provisioner**

Le seguenti funzionalità sono disponibili con la release Astra Control Provisioner 23,10:

- **Protezione backend dello storage avanzata con crittografia Kerberos 5:** È possibile migliorare la protezione dello storage ["attivazione della crittografia"](#) per il traffico tra il cluster gestito e il back-end dello storage. Astra Control Provisioner supporta la crittografia Kerberos 5 su connessioni NFSv4,1 da cluster Red Hat OpenShift a Azure NetApp Files e volumi ONTAP on-premise.
- **Recupera i dati utilizzando uno snapshot:** Astra Control Provisioner fornisce un rapido ripristino dei volumi in-place da uno snapshot utilizzando `TridentActionSnapshotRestore` (TASR) CR.
- **Funzionalità di backup e ripristino per le applicazioni con `ontap-nas-economy` Backend di archiviazione con driver:** Come descritto [sopra](#).

- **Supporto di Astra Control Service per Red Hat OpenShift Service su cluster AWS (ROSA)**

["Aggiungere un cluster"](#)

- **Supporto per la gestione delle applicazioni che utilizzano lo storage NVMe/TCP**

Astra Control è ora in grado di gestire le applicazioni supportate da volumi persistenti connessi tramite NVMe/TCP.

- **I ganci di esecuzione sono disattivati per impostazione predefinita:** A partire da questa release, la funzionalità dei ganci di esecuzione può essere ["attivato"](#) o è disattivato per maggiore protezione (è disattivato per impostazione predefinita). Se non sono ancora stati creati ganci di esecuzione da utilizzare con Astra Control, è necessario ["attivare la funzione ganci di esecuzione"](#) per iniziare a creare ganci. Se sono stati creati dei ganci di esecuzione prima di questa release, la funzionalità dei ganci di esecuzione rimane attivata ed è possibile utilizzare i ganci normalmente.

## 2 ottobre 2023

### Nuove funzionalità e supporto

Si tratta di una versione di correzione dei bug di minore entità.

## 27 luglio 2023

### Nuove funzionalità e supporto

- Le operazioni di cloni ora supportano solo cloni attivi (stato corrente dell'applicazione gestita). Per clonare da uno snapshot o da un backup, utilizzare il flusso di lavoro di ripristino.

["Ripristinare le applicazioni"](#)

## 26 giugno 2023

### Nuove funzionalità e supporto

- Gli abbonamenti a Azure Marketplace vengono fatturati ora anziché al minuto

["Impostare la fatturazione"](#)

## 30 maggio 2023

### Nuove funzionalità e supporto

- Supporto per cluster Amazon EKS privati

["Gestire i cluster privati da Astra Control Service"](#)

- Supporto per la selezione della classe di storage di destinazione durante le operazioni di ripristino o clonazione

["Ripristinare le applicazioni"](#)

## 15 maggio 2023

### Nuove funzionalità e supporto

Si tratta di una versione di correzione dei bug di minore entità.

## 25 aprile 2023

### Nuove funzionalità e supporto

- Supporto per cluster Red Hat OpenShift privati

["Gestire i cluster privati da Astra Control Service"](#)

- Supporto per l'inclusione o l'esclusione delle risorse applicative durante le operazioni di ripristino

["Ripristinare le applicazioni"](#)

- Supporto per la gestione delle applicazioni solo dati

["Inizia a gestire le app"](#)

## 17 gennaio 2023

### Nuove funzionalità e supporto

- Funzionalità migliorata di esecuzione hook con opzioni di filtraggio aggiuntive

["Gestire gli hook di esecuzione delle applicazioni"](#)

- Supporto per NetApp Cloud Volumes ONTAP come back-end per lo storage

["Scopri di più su Astra Control"](#)

## 22 novembre 2022

### Nuove funzionalità e supporto

- Supporto per applicazioni che si estendono su più spazi dei nomi

["Definire le applicazioni"](#)

- Supporto per l'inclusione delle risorse cluster in una definizione applicativa

### "Definire le applicazioni"

- Report avanzati sui progressi delle operazioni di backup, ripristino e clonazione

### "Monitorare le attività in esecuzione"

- Supporto per la gestione di cluster che hanno già una versione compatibile di Astra Trident installata

### "Inizia a gestire i cluster Kubernetes da Astra Control Service"

- Supporto per la gestione di più abbonamenti a provider cloud in un singolo account Astra Control Service

### "Gestire le istanze cloud"

- Supporto per l'aggiunta di cluster Kubernetes autogestiti ospitati in ambienti di cloud pubblico ad Astra Control Service

### "Inizia a gestire i cluster Kubernetes da Astra Control Service"

- La fatturazione per Astra Control Service viene ora misurata per namespace invece che per applicazione

### "Impostare la fatturazione"

- Supporto per l'iscrizione alle offerte basate sui termini di Astra Control Service tramite AWS Marketplace

### "Impostare la fatturazione"

## Problemi noti e limitazioni

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

## 7 settembre 2022

Questa release include miglioramenti di stabilità e resilienza per l'infrastruttura Astra Control Service.

## 10 agosto 2022

Questa versione include le seguenti nuove funzioni e miglioramenti.

- Workflow di gestione delle applicazioni migliorato i flussi di lavoro di gestione delle applicazioni migliorati offrono una maggiore flessibilità nella definizione delle applicazioni gestite da Astra Control.

### "Gestire le applicazioni"

- Supporto per i cluster Amazon Web Services Astra Control Service ora può gestire le applicazioni in esecuzione sui cluster ospitati in Amazon Elastic Kubernetes Service. È possibile configurare i cluster in modo che utilizzino Amazon Elastic Block Store o Amazon FSX per NetApp ONTAP come back-end dello storage.

### "Configurare Amazon Web Services"

- Hook di esecuzione migliorati oltre agli hook di esecuzione pre e post-snapshot, è ora possibile configurare i seguenti tipi di hook di esecuzione:

- Pre-backup
- Post-backup
- Post-ripristino

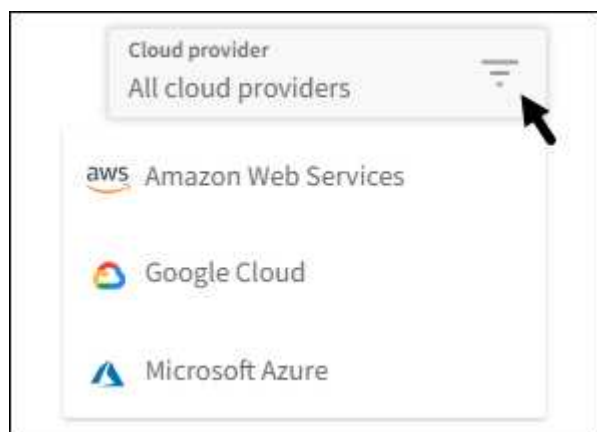
Tra gli altri miglioramenti, Astra Control supporta ora l'utilizzo dello stesso script per più hook di esecuzione.



In questa release sono stati rimossi gli hook di esecuzione predefiniti pre e post-snapshot forniti da NetApp per applicazioni specifiche. Se non fornisci i tuoi hook di esecuzione per le snapshot, Astra Control Service effettuerà snapshot coerenti con il crash solo a partire dal 4 agosto 2022. Visitare il "[Repository NetApp Verda GitHub](#)" per gli script hook di esecuzione di esempio che è possibile modificare per adattarsi al proprio ambiente.

### "Gestire gli hook di esecuzione delle applicazioni"

- Supporto di Azure Marketplace ora puoi iscriverti a Astra Control Service tramite Azure Marketplace.
- Selezione del provider di cloud leggendo la documentazione di Astra Control Service, è ora possibile selezionare il provider di cloud in alto a destra nella pagina. Verrà visualizzata la documentazione relativa solo al cloud provider selezionato.



## 26 aprile 2022

Questa versione include le seguenti nuove funzioni e miglioramenti.

- Namespace RBAC (Role-Based Access Control) Astra Control Service supporta ora l'assegnazione di vincoli di spazio dei nomi agli utenti Member o Viewer.

### "RBAC (role-based access control) dello spazio dei nomi"

- Supporto di Azure Active Directory Astra Control Service supporta i cluster AKS che utilizzano Azure Active Directory per l'autenticazione e la gestione delle identità.

### "Inizia a gestire i cluster Kubernetes da Astra Control Service"

- Supporto per cluster AKS privati è ora possibile gestire cluster AKS che utilizzano indirizzi IP privati.

### "Inizia a gestire i cluster Kubernetes da Astra Control Service"

- Rimozione del bucket da Astra Control è ora possibile rimuovere un bucket da Astra Control Service.

["Rimuovere una benna"](#)

## 14 dicembre 2021

Questa versione include le seguenti nuove funzioni e miglioramenti.

- Nuove opzioni di back-end per lo storage
- Ripristino delle applicazioni in-place è ora possibile ripristinare uno snapshot, un clone o un backup di un'applicazione in uso ripristinando sullo stesso cluster e namespace.

["Ripristinare le applicazioni"](#)

- Eventi di script con hook di esecuzione Astra Control supporta script personalizzati che possono essere eseguiti prima o dopo l'esecuzione di un'istanza di un'applicazione. Ciò consente di eseguire attività come la sospensione delle transazioni del database in modo che l'istanza dell'applicazione di database sia coerente.

["Gestire gli hook di esecuzione delle applicazioni"](#)

- Applicazioni implementate dall'operatore Astra Control supporta alcune applicazioni quando vengono implementate con gli operatori.

["Inizia a gestire le app"](#)

- Entità del servizio con ambito del gruppo di risorse Astra Control Service supporta ora le entità del servizio che utilizzano un ambito del gruppo di risorse.

["Creare un'entità del servizio Azure"](#)

## 5 agosto 2021

Questa versione include le seguenti nuove funzioni e miglioramenti.

- Centro di controllo Astra  
Astra Control è ora disponibile in un nuovo modello di implementazione. *Astra Control Center* è un software a gestione autonoma che puoi installare e utilizzare nel tuo data center, in modo da poter gestire il Lifecycle management delle applicazioni Kubernetes per i cluster Kubernetes on-premise.

Per saperne di più, ["Consultare la documentazione di Astra Control Center"](#).

- Porta il tuo bucket personale ora puoi gestire i bucket che Astra utilizza per backup e cloni aggiungendo bucket aggiuntivi e modificando il bucket predefinito per i cluster Kubernetes nel tuo cloud provider.

["Gestire i bucket"](#)

## 2 giugno 2021

Questa versione include correzioni di bug e i seguenti miglioramenti al supporto di Google Cloud.

- Supporto per VPC condivisi è ora possibile gestire i cluster GKE nei progetti GCP con una configurazione di rete VPC condivisa.



- La dimensione del volume persistente per il tipo di servizio CVS Astra Control Service crea ora volumi persistenti con una dimensione minima di 300 GiB quando si utilizza il tipo di servizio CVS.

["Scopri come Astra Control Service utilizza Cloud Volumes Service per Google Cloud come back-end dello storage per i volumi persistenti"](#).

- Il supporto per sistemi operativi ottimizzati per container è ora supportato con i nodi di lavoro GKE. Oltre al supporto per Ubuntu.

["Scopri di più sui requisiti del cluster GKE"](#).

## 15 aprile 2021

Questa versione include le seguenti nuove funzioni e miglioramenti.

- Supporto per i cluster AKS Astra Control Service è ora in grado di gestire le applicazioni in esecuzione su un cluster Kubernetes gestito in Azure Kubernetes Service (AKS).

["Scopri come iniziare"](#).

- REST API l'API REST di Astra Control è ora disponibile per l'uso. L'API si basa sulle tecnologie moderne e sulle Best practice attuali.

["Scopri come automatizzare la gestione del ciclo di vita dei dati delle applicazioni utilizzando l'API REST"](#).

- L'abbonamento annuale Astra Control Service offre ora un *abbonamento Premium*.

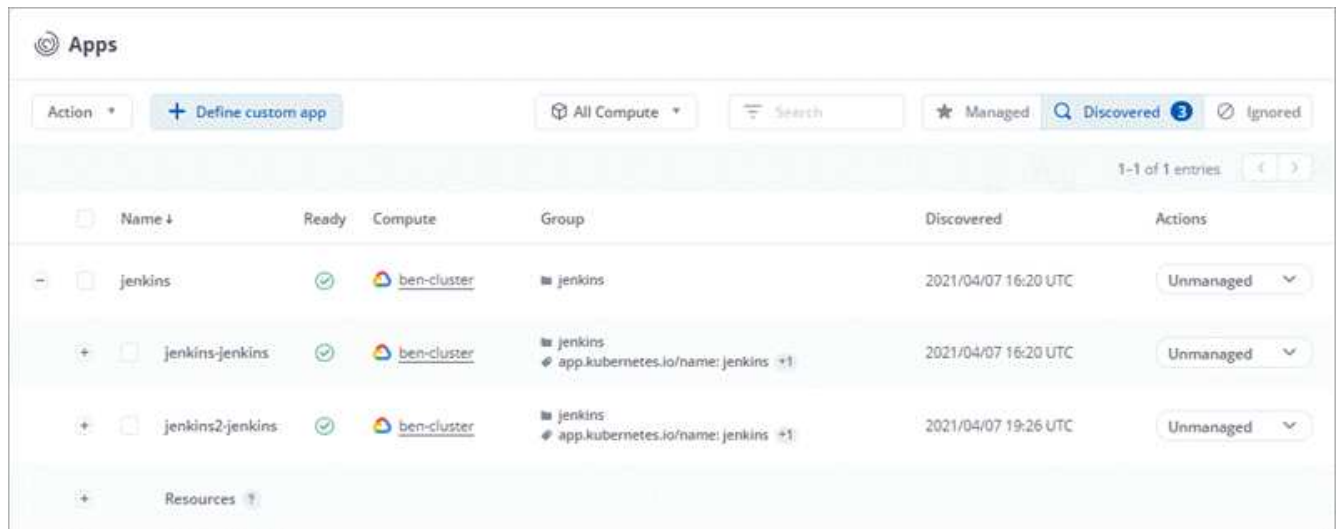
Effettua il pre-pagamento a una tariffa scontata con un abbonamento annuale che ti consente di gestire fino a 10 app per *pacchetto applicativo*. Contatta il reparto vendite NetApp per acquistare tutti i pacchetti necessari per la tua organizzazione, ad esempio acquistando 3 pacchetti per gestire 30 applicazioni da Astra Control Service.

Se gestisci un numero di applicazioni superiore a quello consentito dal tuo abbonamento annuale, ti verrà addebitato un importo di 0.005 dollari al minuto per applicazione (lo stesso di Premium PayGo).

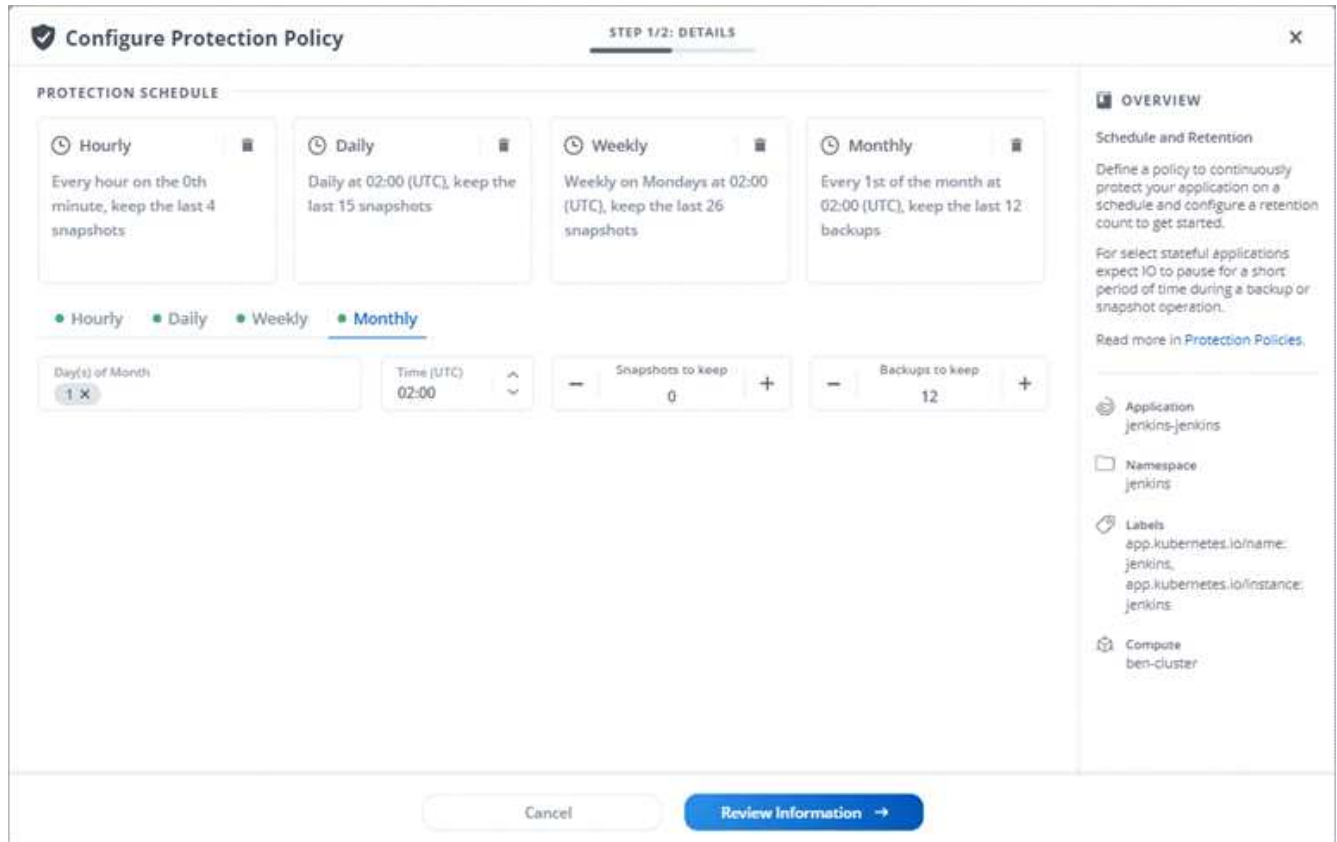
["Scopri di più sui prezzi di Astra Control Service"](#).

- Spazio dei nomi e visualizzazione delle applicazioni abbiamo migliorato la pagina delle applicazioni scoperte per mostrare meglio la gerarchia tra spazi dei nomi e applicazioni. È sufficiente espandere uno spazio dei nomi per visualizzare le applicazioni contenute in tale spazio dei nomi.

["Scopri di più sulla gestione delle app"](#).



- Miglioramenti dell'interfaccia utente le procedure guidate per la protezione dei dati sono state migliorate per una maggiore facilità di utilizzo. Ad esempio, abbiamo perfezionato la procedura guidata dei criteri di protezione per visualizzare più facilmente il programma di protezione definito dall'utente.



- Miglioramenti delle attività abbiamo semplificato la visualizzazione dei dettagli delle attività nel tuo account Astra Control.
  - Filtrare l'elenco delle attività in base all'applicazione gestita, al livello di severità, all'utente e all'intervallo di tempo.
  - Scarica l'attività dell'account Astra Control in un file CSV.
  - Visualizzare le attività direttamente dalla pagina Clusters o dalla pagina Apps dopo aver selezionato un cluster o un'applicazione.

["Scopri di più sulla visualizzazione dell'attività del tuo account"](#).

## 1 marzo 2021

Astra Control Service ora supporta ["CVS tipo di servizio"](#) Con Cloud Volumes Service per Google Cloud. Oltre a supportare già il tipo di servizio *CVS-Performance*. Come promemoria, il servizio di controllo Astra utilizza Cloud Volumes Service per Google Cloud come back-end di storage per i volumi persistenti.

Questo miglioramento significa che Astra Control Service è ora in grado di gestire i dati delle applicazioni per i cluster Kubernetes in esecuzione in *any* ["Area di Google Cloud in cui è supportato Cloud Volumes Service"](#).

Se hai la flessibilità di scegliere tra le aree di Google Cloud, puoi scegliere CVS o CVS-Performance, a seconda dei tuoi requisiti di performance. ["Scopri di più sulla scelta di un tipo di servizio"](#).

## 25 gennaio 2021

Siamo lieti di annunciare che Astra Control Service è ora generalmente disponibile. Abbiamo incluso molti dei feedback ricevuti dalla versione Beta e abbiamo apportato alcuni miglioramenti significativi.

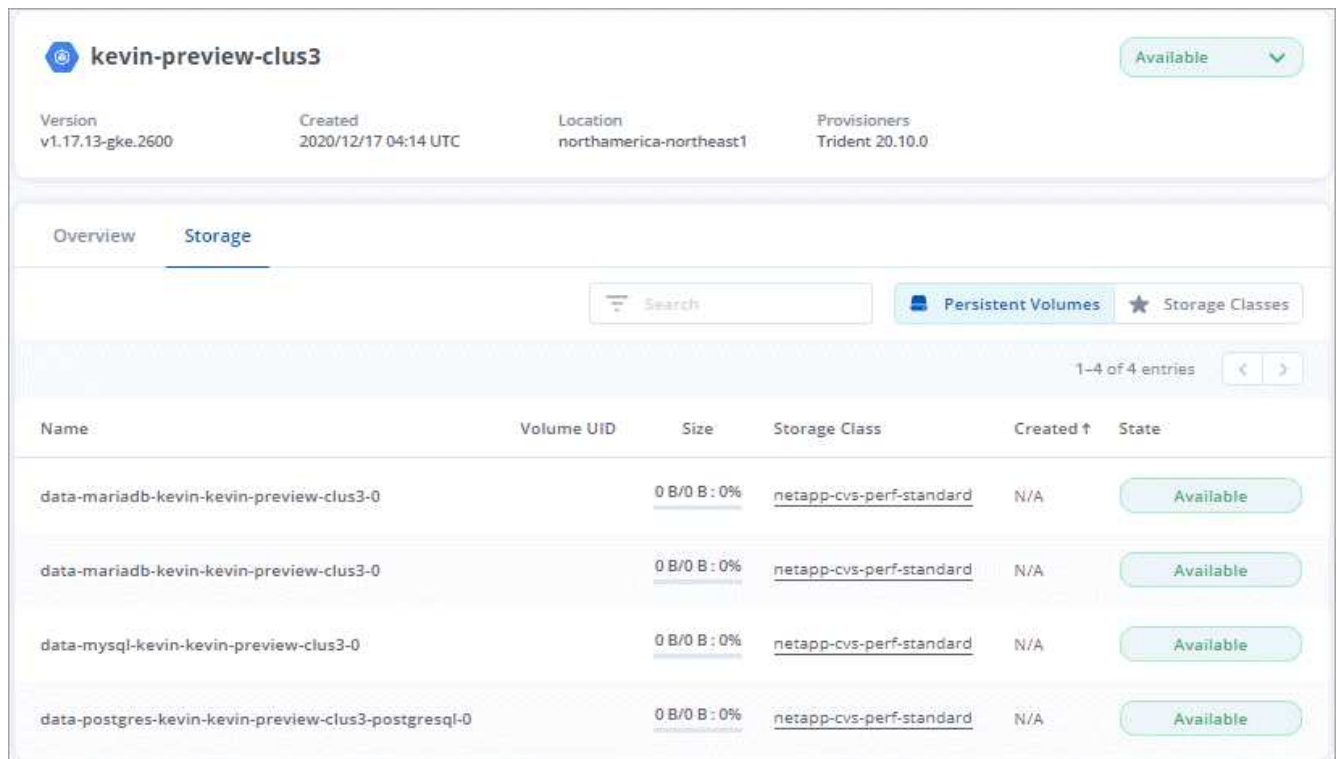
- È ora disponibile la fatturazione, che consente di passare dal piano gratuito al piano Premium. ["Scopri di più sulla fatturazione"](#).
- Astra Control Service ora crea volumi persistenti con una dimensione minima di 100 GiB quando si utilizza il tipo di servizio CVS-Performance.
- Astra Control Service è ora in grado di rilevare le applicazioni più rapidamente.
- È ora possibile creare ed eliminare account da soli.
- Abbiamo migliorato le notifiche quando Astra Control Service non può più accedere a un cluster Kubernetes.

Queste notifiche sono importanti perché Astra Control Service non è in grado di gestire le applicazioni per i cluster disconnessi.

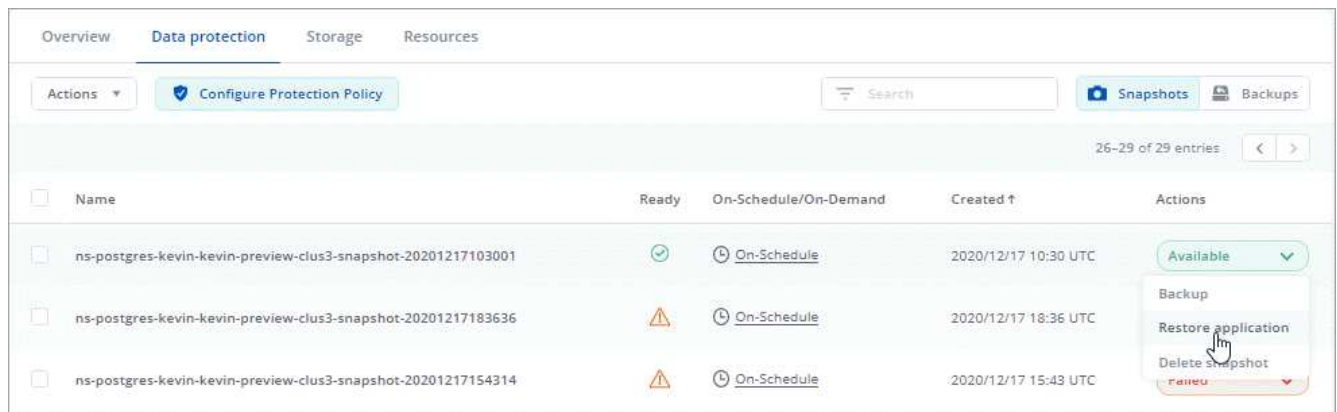
## 17 dicembre 2020 (aggiornamento Beta)

Ci siamo concentrati principalmente sulle correzioni dei bug per migliorare la tua esperienza, ma abbiamo apportato alcuni miglioramenti notevoli:

- Quando si aggiunge il primo calcolo di Kubernetes ad Astra Control Service, l'archivio di oggetti viene ora creato nella regione in cui risiede il cluster.
- I dettagli sui volumi persistenti sono ora disponibili quando si visualizzano i dettagli dello storage a livello di calcolo.



- È stata aggiunta un'opzione per ripristinare un'applicazione da uno snapshot o da un backup esistente.



- Se si elimina un cluster Kubernetes gestito da Astra Control Service, il cluster viene visualizzato in uno stato **removed**. È quindi possibile rimuovere il cluster da Astra Control Service.
- I proprietari degli account possono ora modificare i ruoli assegnati ad altri utenti.
- Abbiamo aggiunto una sezione per la fatturazione, che verrà attivata quando Astra Control Service viene rilasciato per la disponibilità generale (GA).

## 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

- Impossibile definire un'applicazione su uno spazio dei nomi che è stato cancellato e ricreato

### **Backup, ripristino e clonazione**

- I cloni delle applicazioni non riescono a utilizzare una versione specifica di PostgreSQL
- I backup e le snapshot delle applicazioni non vengono eseguiti se la classe `volumesnapshotclass` viene aggiunta dopo la gestione di un cluster
- Il ripristino da un backup quando si utilizza la crittografia in-flight Kerberos può non riuscire
- I dati di backup rimangono nel bucket dopo l'eliminazione per bucket con criteri di conservazione scaduti

### **Altri problemi**

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

## **Impossibile definire un'applicazione su uno spazio dei nomi che è stato cancellato e ricreato**

Se si definisce un'applicazione con uno spazio dei nomi, si elimina lo spazio dei nomi e si reinstalla l'applicazione nello stesso spazio dei nomi, l'operazione non riesce e viene visualizzato un codice di errore 409. Per definire l'applicazione utilizzando lo spazio dei nomi ricreato, eliminare prima la vecchia istanza dell'applicazione.

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

In questo scenario, i backup e le snapshot non vengono eseguiti correttamente e viene visualizzato un errore UI 500. Come soluzione, aggiornare l'elenco delle applicazioni.

## **Il ripristino da un backup quando si utilizza la crittografia in-flight Kerberos può non riuscire**

Quando si ripristina un'applicazione da un backup a un backend di storage che utilizza la crittografia in-flight Kerberos, l'operazione di ripristino potrebbe non riuscire. Questo problema non influisce sul ripristino da uno snapshot o sulla replica dei dati dell'applicazione tramite SnapMirror di NetApp.



Quando si utilizza la crittografia in-flight Kerberos con volumi NFSv4, assicurarsi che i volumi NFSv4 stiano utilizzando le impostazioni corrette. Consultare la sezione Configurazione di dominio NetApp NFSv4 (pagina 13) della ["Guida ai miglioramenti e alle Best practice di NetApp NFSv4"](#).

## **I dati di backup rimangono nel bucket dopo l'eliminazione per bucket con criteri di conservazione scaduti**

Se elimini il backup immutabile di un'app dopo che il criterio di conservazione del bucket è scaduto, il backup viene eliminato da Astra Control ma non dal bucket. Questo problema verrà risolto in una prossima release.

## **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.

## **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 generali**

Le seguenti limitazioni influiscono sulla gestione dei cluster Kubernetes da parte di Astra Control Service in qualsiasi implementazione di Kubernetes supportata.

#### **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 Service 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.

#### **La pagina Activity (attività) visualizza fino a 100,000 eventi**

La pagina Astra Control Activity (attività di controllo Astra) può visualizzare fino a 100,000 eventi. Per visualizzare tutti gli eventi registrati, recuperare gli eventi utilizzando "[API REST di Astra Control](#)".

### **Limitazioni per la gestione dei cluster GKE**

Le seguenti limitazioni si applicano alla gestione dei cluster Kubernetes in Google Kubernetes Engine (GKE).

### **Limitazioni della gestione delle applicazioni**

Le seguenti limitazioni influiscono sulla gestione delle applicazioni da parte di Astra Control Service.

#### **Le operazioni di ripristino in-place alle classi di storage economiche ontap-nas falliscono**

Se si esegue un ripristino sul posto di un'applicazione (ripristinando l'applicazione nello spazio dei nomi originale) e la classe di archiviazione dell'applicazione utilizza `ontap-nas-economy` driver, l'operazione di ripristino può non riuscire se la directory dello snapshot non è nascosta. Prima di eseguire il ripristino sul posto, seguire le istruzioni riportate in "[Abilita backup e ripristino per le operazioni economiche a ontap-nas](#)" per nascondere la directory dell'istantanea.

#### **Non è possibile ripristinare collettivamente più applicazioni che utilizzano lo stesso namespace in un namespace diverso**

Se si gestiscono più applicazioni che utilizzano lo stesso 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.

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

Questa versione di Astra Control Service 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.

## 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.

## 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"](#)



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 tolta. 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"](#)

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.



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.

## Limitazioni RBAC (Role-Based Access Control)

Le seguenti limitazioni si applicano al modo in cui Astra Control limita l'accesso degli utenti alle risorse o alle funzionalità.

## **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 utente membro con vincoli dello spazio dei nomi non può accedere alle applicazioni clonate o ripristinate fino a quando un utente 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. Dopo che un'operazione di clonazione o ripristino crea un nuovo spazio dei nomi, 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.

## **Gli snapshot potrebbero non funzionare per i cluster Kubernetes 1.25 o versioni successive con determinate versioni di snapshot controller**

Le snapshot per i cluster Kubernetes che eseguono la versione 1.25 o successiva possono non riuscire se sul cluster è installata la versione v1beta1 delle API del controller di snapshot.

Per risolvere il problema, eseguire le seguenti operazioni quando si aggiornano le installazioni esistenti di Kubernetes 1.25 o versioni successive:

1. Rimuovere tutti gli Snapshot CRD esistenti e tutti gli snapshot controller esistenti.
2. ["Disinstallare Astra Trident"](#).
3. ["Installare gli snapshot CRD e lo snapshot controller"](#).
4. ["Installare la versione più recente di Astra Trident"](#).
5. ["Creare una classe VolumeSnapshotClass"](#).



## Informazioni sul copyright

Copyright © 2024 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.