Note di rilascio

Astra Control Center

NetApp
August 11, 2025

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"

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.

15 marzo 2024 (24.02.0)

Nuove funzionalità e supporto

- **Distribuire Astra Control Center senza un registro privato**: Non è più necessario trasferire le immagini Astra Control Center in un registro privato o utilizzarne una come parte dell'ambiente Astra Control.
- **Correzioni di bug minori**

Problemi noti e limitazioni

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

(Anteprima tecnica) flussi di lavoro Kubernetes dichiarativi

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

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 (23.10.0)

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".

- **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 Provivisioner 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 Provivisioner fornisce un rapido ripristino dei volumi in-place da uno snapshot utilizzando `TridentActionSnapshotRestore` (TASR) CR.
    - **Miglioramenti di SnapMirror**: Utilizzare la funzionalità di replica delle app in ambienti in cui Astra Control non dispone di connettività diretta a un cluster ONTAP o di accesso alle credenziali ONTAP. Questa funzionalità ti consente di utilizzare la replica senza dover gestire un backend dello storage o le sue credenziali in Astra Control.
    - **Funzionalità di backup e ripristino per le applicazioni con `ontap-nas-economy` Backend di archiviazione con driver**: Come descritto sopra.
- **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.

Problemi noti e limitazioni

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

31 luglio 2023 (23.07.0)

Nuove funzionalità e supporto

- "Supporto per l'utilizzo di NetApp MetroCluster in una configurazione stretch come backend di storage"
- "Supporto per l'utilizzo di Longhorn come backend di storage"

- "È ora possibile replicare le applicazioni tra backend ONTAP dallo stesso cluster Kubernetes"
- "Astra Control Center ora supporta 'userPrincipalName' come attributo di login alternativo per gli utenti remoti (LDAP)"
- "Il nuovo tipo di gancio di esecuzione "post-failover" può essere eseguito dopo il failover della replica con Astra Control Center"
- I flussi di lavoro clonati ora supportano solo i cloni live (lo stato corrente dell'applicazione gestita). Per clonare da uno snapshot o da un backup, utilizzare "ripristinare il flusso di lavoro".

Problemi noti e limitazioni

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

18 maggio 2023 (23.04.2)

Questa patch release (23.04.2) per Astra Control Center (23.04.0) fornisce supporto per "Kubernetes CSI snapshotter esterno v6.1.0" e corregge quanto segue:

- Un bug con il ripristino delle applicazioni in-place quando si utilizzano gli hook di esecuzione
- Problemi di connessione con il servizio bucket

25 aprile 2023 (23.04.0)

Nuove funzionalità e supporto

- "Licenza di valutazione di 90 giorni abilitata per impostazione predefinita per le nuove installazioni di Astra Control Center"
- "Funzionalità migliorata di esecuzione hook con opzioni di filtraggio aggiuntive"
- "È ora possibile eseguire gli hook di esecuzione dopo il failover della replica con Astra Control Center"
- "Supporto per la migrazione dei volumi dalla classe di storage 'ontap-nas-Economy' alla classe di storage 'ontap-nas'"
- "Supporto per l'inclusione o l'esclusione delle risorse applicative durante le operazioni di ripristino"
- "Supporto per la gestione delle applicazioni solo dati"

Problemi noti e limitazioni

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

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)

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)

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)

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)

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:

- I backup e le snapshot delle applicazioni non vengono eseguiti se la classe volumesnapshotclass viene aggiunta dopo la gestione di un cluster
- La gestione di un cluster con Astra Control Center non riesce quando il file kubeconfig contiene più di un contesto
- 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 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

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.

La gestione di un cluster con Astra Control Center non riesce quando il file kubeconfig 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.

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.

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.

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
- I vincoli di ruolo restrittivi possono essere ignorati per le risorse su cluster non di connettori

Limitazioni della gestione delle applicazioni

- Non è possibile ripristinare collettivamente più applicazioni in un singolo namespace in un namespace diverso
- Astra Control non supporta applicazioni che utilizzano più classi di storage per spazio dei nomi
- 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
- Gli snapshot potrebbero non funzionare per i cluster Kubernetes 1.25 o versioni successive con determinate versioni di snapshot controller
- I backup e le snapshot potrebbero non essere conservati durante la rimozione di un'istanza di Astra Control Center
- Le operazioni di ripristino in-place alle classi di storage economiche ontap-nas falliscono

Limitazioni generali

- Limitazioni di utenti e gruppi LDAP
- 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
- La pagina Activity (attività) visualizza fino a 100000 eventi
- SnapMirror non supporta le applicazioni che utilizzano NVMe su TCP per backend di storage

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. 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.

I vincoli di ruolo restrittivi possono essere ignorati per le risorse su cluster non di connettori

- **Se le risorse a cui si accede appartengono ai cluster in cui è installato l'ultimo connettore Astra**: Quando a un utente vengono assegnati più ruoli tramite l'appartenenza al gruppo LDAP, i vincoli dei ruoli vengono combinati. Ad esempio, se un utente con un ruolo Visualizzatore locale unisce tre gruppi associati al ruolo membro, l'utente dispone ora dell'accesso al ruolo Visualizzatore alle risorse originali e dell'accesso al ruolo membro alle risorse acquisite tramite l'appartenenza al gruppo.
- **Se le risorse a cui si accede appartengono ai cluster che non hanno Astra Connector installato**: Quando a un utente vengono assegnati più ruoli tramite l'appartenenza al gruppo LDAP, i vincoli del ruolo più permissivo sono gli unici che hanno effetto.

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 supporta applicazioni che utilizzano più classi di storage per spazio dei nomi

Astra Control supporta applicazioni che utilizzano una singola classe di storage per spazio dei nomi. Quando Aggiungi un'applicazione a uno spazio dei nomi, assicurati che l'applicazione abbia la stessa classe di storage delle altre applicazioni nello spazio dei nomi.

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, fare riferimento a. "Requisiti di Astra Control Center".

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".

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.

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.

Limitazioni di utenti e gruppi LDAP

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

Astra Control non supporta un'entità LDAP (utente o gruppo) con un DN contenente un RDN con uno spazio finale o finale.

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.

La pagina Activity (attività) visualizza fino a 100000 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 di controllo Astra".

SnapMirror non supporta le applicazioni che utilizzano NVMe su TCP per backend di storage

Astra Control Center non supporta la replica SnapMirror di NetApp per backend di storage che utilizzano il protocollo NVMe over TCP.

Trova ulteriori informazioni

- "Problemi noti"