



Utilizzare Astra

Astra Control Center

NetApp
November 20, 2023

Sommario

- Utilizzare Astra 1
 - Gestire le applicazioni 1
 - Proteggi le app 7
 - Visualizzare lo stato delle applicazioni e del cluster 14
 - Gestisci il tuo account 16
 - Gestire i bucket 22
 - Gestire il back-end dello storage 23
 - Monitorare e proteggere l'infrastruttura 25
 - Aggiornare una licenza esistente 32
 - Annulla la gestione di app e cluster 33
 - Disinstallare Astra Control Center 34

Utilizzare Astra

Gestire le applicazioni

Inizia a gestire le app

Dopo di lei ["Aggiungere un cluster alla gestione di Astra Control"](#), È possibile installare le applicazioni sul cluster (al di fuori di Astra Control), quindi andare alla pagina Apps (applicazioni) in Astra Control per iniziare a gestire le applicazioni e le relative risorse.

Installa le app sul tuo cluster

Una volta aggiunto il cluster ad Astra Control, è possibile installare le applicazioni o gestire quelle esistenti sul cluster. È possibile gestire qualsiasi applicazione con ambito per uno spazio dei nomi. Una volta che i pod sono online, puoi gestire l'applicazione con Astra Control.

Per assistenza nell'implementazione delle applicazioni validate dai grafici Helm, fare riferimento a quanto segue:

- ["Implementare MariaDB da un grafico Helm"](#)
- ["Implementa MySQL da un grafico Helm"](#)
- ["Implementare Postgres da un grafico Helm"](#)
- ["Implementare Jenkins da un grafico Helm"](#)

Gestire le applicazioni

Astra Control consente di gestire le applicazioni a livello di spazio dei nomi o in base all'etichetta Kubernetes.



Le app implementate con Helm 2 non sono supportate.

Per gestire le applicazioni, è possibile eseguire le seguenti attività:

- Gestire le applicazioni
 - [Gestire le applicazioni in base allo spazio dei nomi](#)
 - [Gestisci le app in base all'etichetta Kubernetes](#)
- [Ignorare le applicazioni](#)
- [Annulla gestione delle applicazioni](#)



Astra Control non è un'applicazione standard, ma un'applicazione di sistema. Non si dovrebbe tentare di gestire Astra Control da solo. Per impostazione predefinita, Astra Control non viene visualizzato per la gestione. Per visualizzare le applicazioni di sistema, utilizza il filtro "Mostra app di sistema".

Per istruzioni su come gestire le applicazioni utilizzando l'API Astra, vedere ["Astra Automation e informazioni API"](#).



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. L'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.

Gestire le applicazioni in base allo spazio dei nomi

La sezione **scoperta** della pagina App mostra gli spazi dei nomi e le applicazioni installate da Helm o personalizzate in tali spazi dei nomi. Puoi scegliere di gestire ogni applicazione singolarmente o a livello di spazio dei nomi. Tutto questo si riduce al livello di granularità necessario per le operazioni di protezione dei dati.

Ad esempio, è possibile impostare una policy di backup per "maria" con cadenza settimanale, ma potrebbe essere necessario eseguire il backup di "mariadb" (che si trova nello stesso namespace) con maggiore frequenza. In base a tali esigenze, sarebbe necessario gestire le applicazioni separatamente e non in un singolo namespace.

Mentre Astra Control consente di gestire separatamente entrambi i livelli della gerarchia (lo spazio dei nomi e le applicazioni in tale spazio dei nomi), la procedura migliore è scegliere uno o l'altro. Le azioni eseguite in Astra Control possono non riuscire se vengono eseguite contemporaneamente sia a livello di spazio dei nomi che di applicazione.

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Apps** (applicazioni).
2. Selezionare **rilevato**.

Apps						
Actions		+ Define		All Clusters	Search	Managed Discovered 54 Ignored
	Name	Ready	Cluster	Group	Discovered	Actions
<input type="checkbox"/>	default			grp_default	2021/06/28 17:36 UTC	Managed
<input type="checkbox"/>	default1			grp1_default	2021/06/28 17:36 UTC	Unmanaged
<input type="checkbox"/>	default2			grp2_default	2021/06/28 17:36 UTC	Unmanaged
<input type="checkbox"/>	netapp-acc-operator			netapp-acc-operator	2021/07/13 12:36 UTC	Unmanaged
<input type="checkbox"/>	pcloud			pcloud	2021/07/13 12:37 UTC	Unmanaged

3. Visualizzare l'elenco degli spazi dei nomi rilevati. Espandere lo spazio dei nomi per visualizzare le applicazioni e le risorse associate.

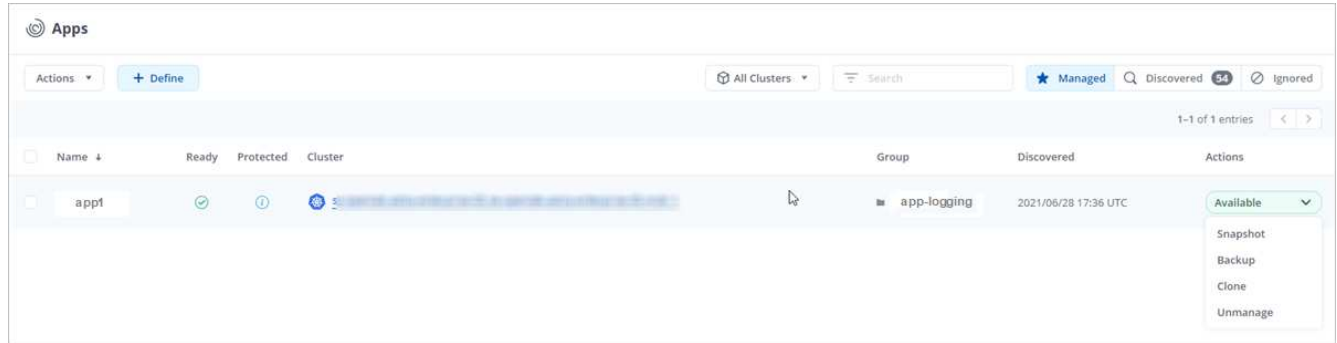
Astra Control mostra le applicazioni Helm e le applicazioni con etichetta personalizzata nello spazio dei nomi. Se le etichette Helm sono disponibili, sono contrassegnate da un'icona di tag.

4. Esaminare la colonna **Gruppo** per visualizzare lo spazio dei nomi in cui viene eseguita l'applicazione (indicato con l'icona della cartella).
5. Decidere se si desidera gestire ciascuna applicazione singolarmente o a livello di spazio dei nomi.
6. Individuare l'applicazione desiderata al livello desiderato nella gerarchia e dal menu Actions (azioni), selezionare **Manage** (Gestisci).

7. Se non si desidera gestire un'applicazione, dal menu Actions (azioni) accanto all'applicazione, selezionare **Ignore** (Ignora).

Ad esempio, se si desidera gestire tutte le applicazioni nello spazio dei nomi "maria" insieme in modo che abbiano le stesse policy di backup e snapshot, è necessario gestire lo spazio dei nomi e ignorare le applicazioni nello spazio dei nomi.

8. Per visualizzare l'elenco delle applicazioni gestite, selezionare **Managed** come filtro di visualizzazione.



Notare che l'applicazione appena aggiunta presenta un'icona di avviso sotto la colonna Protected, che indica che il backup non è stato ancora eseguito e non è stato pianificato per i backup.

9. Per visualizzare i dettagli di una particolare applicazione, selezionare il nome dell'applicazione.

Risultato

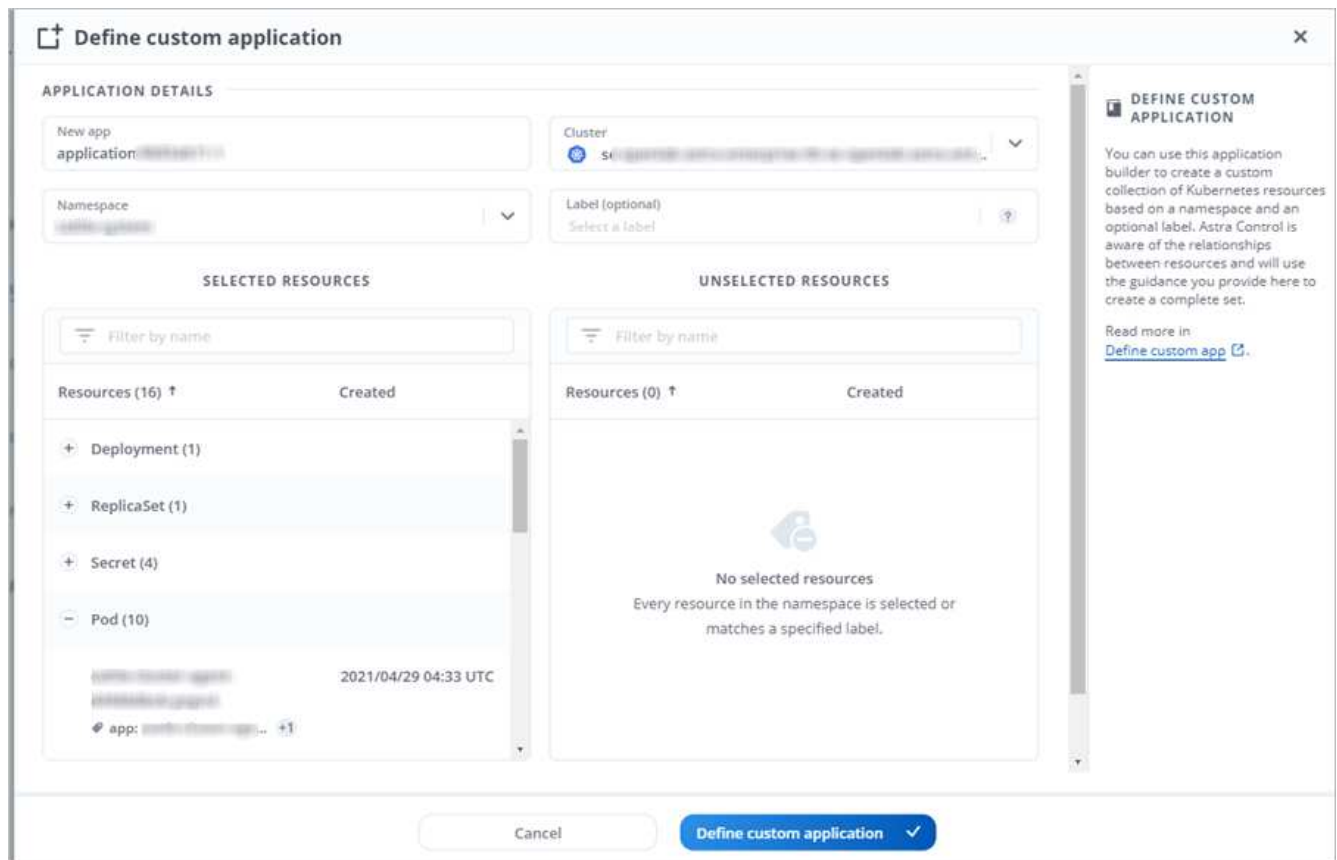
Le applicazioni che hai scelto di gestire sono ora disponibili nella scheda **Managed**. Tutte le applicazioni ignorate verranno spostate nella scheda **ignored**. Idealmente, la scheda scoperta non mostra alcuna applicazione, in modo che, una volta installate, siano più facili da trovare e gestire.

Gestisci le app in base all'etichetta Kubernetes

Astra Control include un'azione nella parte superiore della pagina Apps denominata **define custom app**. Puoi utilizzare questa azione per gestire le app identificate con un'etichetta Kubernetes. ["Scopri di più sulla definizione di applicazioni personalizzate con l'etichetta Kubernetes"](#).

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Apps** (applicazioni).
2. Selezionare **Definisci**.



3. Nella finestra di dialogo **Definisci applicazione personalizzata**, fornire le informazioni necessarie per gestire l'applicazione:
 - a. **Nuova applicazione**: Immettere il nome visualizzato dell'applicazione.
 - b. **Cluster**: Selezionare il cluster in cui risiede l'applicazione.
 - c. **Namespace**: selezionare lo spazio dei nomi dell'applicazione.
 - d. **Label**: inserire un'etichetta o selezionare un'etichetta dalle risorse sottostanti.
 - e. **Risorse selezionate**: Consente di visualizzare e gestire le risorse Kubernetes selezionate che si desidera proteggere (pod, segreti, volumi persistenti e altro ancora).
 - Visualizzare le etichette disponibili espandendo una risorsa e facendo clic sul numero di etichette.
 - Selezionare una delle etichette.

Dopo aver scelto un'etichetta, questa viene visualizzata nel campo **etichetta**. Astra Control aggiorna anche la sezione **risorse non selezionate** per mostrare le risorse che non corrispondono all'etichetta selezionata.
 - f. **Risorse non selezionate**: Verifica le risorse dell'app che non desideri proteggere.
4. Fare clic su **Definisci applicazione personalizzata**.

Risultato

Astra Control consente la gestione dell'applicazione. A questo punto, è possibile trovarlo nella scheda **Managed**.

Ignorare le applicazioni

Se un'applicazione è stata rilevata, viene visualizzata nell'elenco rilevato. In questo caso, è possibile pulire l'elenco scoperto in modo che le nuove applicazioni appena installate siano più facili da trovare. Oppure, potresti avere applicazioni che gestisci e decidere in seguito di non doverle più gestire. Se non si desidera gestire queste applicazioni, è possibile indicare che devono essere ignorate.

Inoltre, è possibile gestire le applicazioni in un unico namespace insieme (gestito dallo spazio dei nomi). È possibile ignorare le applicazioni che si desidera escludere dallo spazio dei nomi.

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Apps** (applicazioni).
2. Selezionare **rilevato** come filtro.
3. Selezionare l'applicazione.
4. Dal menu Actions (azioni), selezionare **Ignore** (Ignora).
5. Per non ignorare, dal menu azioni, selezionare **Unignore**.

Annulla gestione delle applicazioni

Quando non si desidera più eseguire il backup, lo snapshot o la clonazione di un'applicazione, è possibile interromperne la gestione.



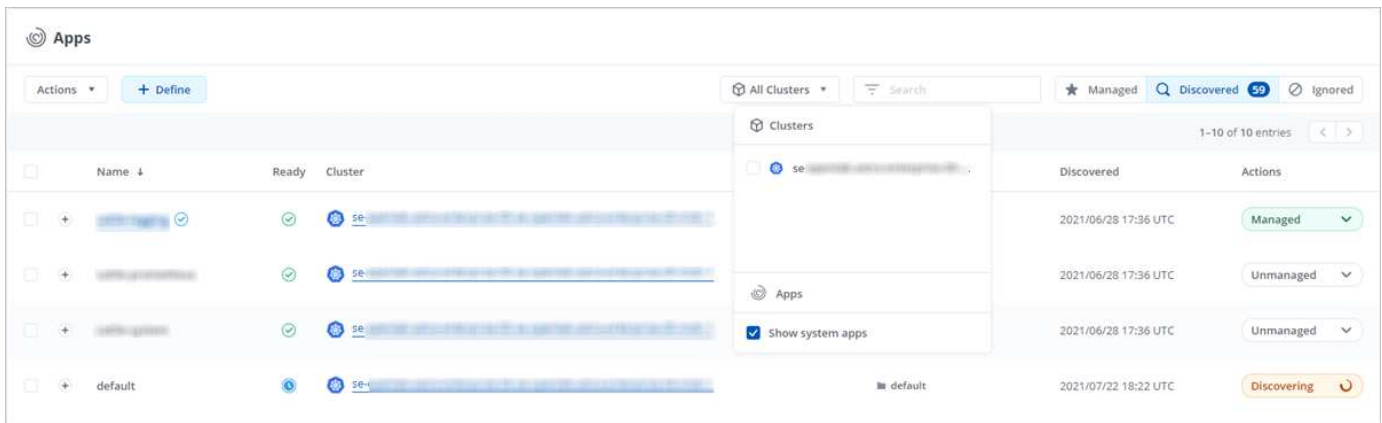
Se si annulla la gestione di un'applicazione, i backup o le snapshot creati in precedenza andranno persi.

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Apps** (applicazioni).
2. Selezionare **Managed** come filtro.
3. Selezionare l'applicazione.
4. Dal menu Actions (azioni), selezionare **UnManage** (Annulla gestione).
5. Esaminare le informazioni.
6. Digitare "unManage" per confermare.
7. Selezionare **Sì, Annulla gestione applicazione**.

E le applicazioni di sistema?

Astra Control rileva anche le applicazioni di sistema in esecuzione su un cluster Kubernetes. È possibile visualizzare le applicazioni di sistema selezionando la casella di controllo **Mostra applicazioni di sistema** sotto il filtro cluster nella barra degli strumenti.



Per impostazione predefinita, queste applicazioni di sistema non vengono visualizzate perché è raro che sia necessario eseguirne il backup.



Astra Control non è un'applicazione standard, ma un'applicazione di sistema. Non si dovrebbe tentare di gestire Astra Control da solo. Per impostazione predefinita, Astra Control non viene visualizzato per la gestione. Per visualizzare le applicazioni di sistema, utilizza il filtro "Mostra app di sistema".

Trova ulteriori informazioni

- ["Utilizzare l'API Astra"](#)

Definire un esempio di applicazione personalizzata

La creazione di un'applicazione personalizzata consente di raggruppare gli elementi del cluster Kubernetes in una singola applicazione.

Un'applicazione personalizzata ti offre un controllo più granulare su ciò che devi includere in un'operazione Astra Control, tra cui:

- Clonare
- Snapshot
- Backup
- Policy di protezione

Nella maggior parte dei casi, è consigliabile utilizzare le funzionalità di Astra Control sull'intera applicazione. Tuttavia, è anche possibile creare un'applicazione personalizzata per utilizzare queste funzionalità tramite le etichette assegnate agli oggetti Kubernetes in uno spazio dei nomi.

Per creare un'applicazione personalizzata, accedere alla pagina App e fare clic su **+ Definisci**.

Durante le selezioni, la finestra Custom App mostra le risorse che verranno incluse o escluse dall'applicazione personalizzata. Questo ti aiuta a scegliere i criteri corretti per la definizione della tua applicazione personalizzata.



Le applicazioni personalizzate possono essere create solo all'interno di uno spazio dei nomi specificato in un singolo cluster. Astra Control non supporta la capacità di un'applicazione personalizzata di includere più spazi dei nomi o cluster.

Un'etichetta è una coppia chiave/valore che è possibile assegnare agli oggetti Kubernetes per l'identificazione. Le etichette semplificano l'ordinamento, l'organizzazione e la ricerca degli oggetti Kubernetes. Per ulteriori informazioni sulle etichette Kubernetes, "[Consulta la documentazione ufficiale di Kubernetes](#)".



La sovrapposizione di policy per la stessa risorsa con nomi diversi può causare conflitti di dati. Se crei un'applicazione personalizzata per una risorsa, assicurati che non venga clonata o sottoposta a backup in base ad altre policy.

Esempio: Policy di protezione separata per la release canary

In questo esempio, il team devops sta gestendo un'implementazione di release canary. Il cluster dispone di tre pod che eseguono nginx. Due dei pod sono dedicati al rilascio stabile. Il terzo pod è per la release canary.

L'amministratore Kubernetes del team devops aggiunge l'etichetta `deployment=stable` ai pod a rilascio stabile. Il team aggiunge l'etichetta `deployment=canary` al pod di rilascio canary.

La release stabile del team include un requisito per snapshot orarie e backup giornalieri. La release canary è più effimera, quindi vogliono creare una politica di protezione meno aggressiva e a breve termine per qualsiasi cosa etichettata `deployment=canary`.

Per evitare possibili conflitti di dati, l'amministratore creerà due applicazioni personalizzate: Una per la release canary e una per la release stabile. In questo modo i backup, gli snapshot e le operazioni di clonazione vengono separati per i due gruppi di oggetti Kubernetes.

Fasi

1. Dopo che il team ha aggiunto il cluster ad Astra Control, il passaggio successivo consiste nella definizione di un'applicazione personalizzata. A tale scopo, il team fa clic sul pulsante **+ Definisci** nella pagina App.
2. Nella finestra a comparsa che viene visualizzata, il raggruppamento viene impostato `devops-canary-deployment` come nome dell'applicazione. Il team sceglie il cluster nell'elenco a discesa **Cluster**, quindi lo spazio dei nomi dell'applicazione dall'elenco a discesa **namespace**.
3. Il team può digitare entrambi i tipi `deployment=canary` Nel campo **etichette**, oppure selezionare l'etichetta dalle risorse elencate di seguito.
4. Dopo aver definito l'applicazione personalizzata per l'implementazione canary, il team ripete il processo per l'implementazione stabile.

Una volta terminata la creazione delle due applicazioni personalizzate, il team può trattare queste risorse come qualsiasi altra applicazione Astra Control. Possono clonarli, creare backup e snapshot e creare una policy di protezione personalizzata per ciascun gruppo di risorse in base alle etichette Kubernetes.

Proteggi le app

Proteggi le app con snapshot e backup

Proteggi le tue applicazioni eseguendo snapshot e backup utilizzando una policy di protezione automatica o ad-hoc. È possibile utilizzare l'interfaccia utente Astra o "[L'API Astra](#)" per proteggere le applicazioni.



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. Le app implementate con Helm 2 non sono supportate.



Quando crei un progetto per ospitare un'applicazione su un cluster OpenShift, al progetto (o namespace Kubernetes) viene assegnato un UID SecurityContext. Per consentire ad Astra Control Center di proteggere la tua applicazione e spostarla in un altro cluster o progetto in OpenShift, devi aggiungere policy che consentano all'applicazione di essere eseguita come qualsiasi UID. Ad esempio, i seguenti comandi CLI di OpenShift concedono le policy appropriate a un'applicazione WordPress.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

Snapshot e backup

Una *snapshot* è una copia point-in-time di un'applicazione memorizzata sullo stesso volume fornito dell'applicazione. Di solito sono veloci. Gli snapshot locali vengono utilizzati per ripristinare l'applicazione a un punto precedente. Le snapshot sono utili per cloni veloci; le snapshot includono tutti gli oggetti Kubernetes per l'applicazione, inclusi i file di configurazione.

Un *backup* viene memorizzato nell'archivio di oggetti esterno. Un backup può essere più lento rispetto agli snapshot locali. È possibile migrare un'applicazione ripristinando il backup su un cluster diverso. È inoltre possibile scegliere un periodo di conservazione più lungo per i backup.



Non è possibile essere completamente protetti fino a quando non si dispone di un backup recente. Ciò è importante perché i backup vengono memorizzati in un archivio a oggetti lontano dai volumi persistenti. Se un guasto o un incidente cancella il cluster e lo storage persistente, è necessario un backup per il ripristino. Un'istantanea non ti consentirebbe di ripristinarla.

Configurare un criterio di protezione

Una policy di protezione protegge un'applicazione creando snapshot, backup o entrambi in base a una pianificazione definita. È possibile scegliere di creare snapshot e backup ogni ora, ogni giorno, ogni settimana e ogni mese, nonché specificare il numero di copie da conservare.

Fasi

1. Fare clic su **Apps** (applicazioni), quindi sul nome di un'applicazione.
2. Fare clic su **Data Protection** (protezione dati).
3. Fare clic su **Configura policy di protezione**.
4. Definire un programma di protezione scegliendo il numero di snapshot e backup da conservare ogni ora, ogni giorno, ogni settimana e ogni mese.

È possibile definire le pianificazioni orarie, giornaliere, settimanali e mensili contemporaneamente. Un programma non diventa attivo fino a quando non viene impostato un livello di conservazione.

Nell'esempio seguente vengono impostati quattro programmi di protezione: ogni ora, ogni giorno, ogni settimana e ogni mese per snapshot e backup.

Configure protection policy

STEP 1/2: DETAILS

✕

PROTECTION SCHEDULE

🕒 Hourly

Every hour on the 0th minute, keep the last 4 snapshots

🕒 Daily

Daily at 02:00 (UTC), keep the last 15 snapshots

🕒 Weekly

Weekly on Mondays at 02:00 (UTC), keep the last 26 snapshots

🕒 Monthly

Every 1st of the month at 02:00 (UTC), keep the last 12 backups

● Hourly

● Daily

● **Weekly**

● Monthly

Select Weekday(s) (optional)

Monday X

Time (UTC) (optional)

02:00

– Snapshots to keep +

26

– Backups to keep +

0

BACKUP DESTINATION

Bucket

ntp-nautilus-bucket-10 - ntp-nautilus-bucket-10

Default

OVERVIEW

Schedule and retention

Define a policy to continuously protect your application on a schedule and configure a retention count to get started.

For select stateful applications, expect I/O to pause for a short time during a backup or snapshot operation.

Read more in [Protection policies](#)

Application

cattle-logging

Namespace

cattle-logging

Cluster

se-openlab-astra-enterprise-05-se-openlab-astra-enterprise-05-mstr-1

Cancel

Review →

5. Fare clic su **Review** (Rivedi).

6. Fare clic su **Set Protection Policy (Imposta policy di protezione)**.

Risultato

Astra Control Center implementa la policy di protezione dei dati creando e conservando snapshot e backup utilizzando i criteri di pianificazione e conservazione definiti dall'utente.

Creare un'istantanea

Puoi creare uno snapshot on-demand in qualsiasi momento.

Fasi

1. Fare clic su **Apps** (applicazioni).
2. Fare clic sull'elenco a discesa nella colonna **azioni** dell'applicazione desiderata.
3. Fare clic su **Snapshot**.
4. Personalizzare il nome dell'istantanea, quindi fare clic su **Review** (Rivedi).
5. Esaminare il riepilogo dell'istantanea e fare clic su **Snapshot**.

Risultato

Viene avviato il processo di snapshot. Un'istantanea viene eseguita correttamente quando lo stato è **Available** nella colonna **Actions** nella pagina **Data Protection > Snapshots**.

Creare un backup

Puoi anche eseguire il backup di un'applicazione in qualsiasi momento.

9



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.

Fasi

1. Fare clic su **Apps** (applicazioni).
2. Fare clic sull'elenco a discesa nella colonna **azioni** dell'applicazione desiderata.
3. Fare clic su **Backup**.
4. Personalizzare il nome del backup.
5. Scegliere se eseguire il backup dell'applicazione da uno snapshot esistente. Se si seleziona questa opzione, è possibile scegliere da un elenco di snapshot esistenti.
6. Scegliere una destinazione per il backup selezionandola dall'elenco dei bucket di storage.
7. Fare clic su **Review** (Rivedi).
8. Esaminare il riepilogo del backup e fare clic su **Backup**.

Risultato

Astra Control Center crea un backup dell'applicazione.



Se la rete presenta un'interruzione o è eccessivamente lenta, potrebbe verificarsi un timeout dell'operazione di backup. In questo modo, il backup non viene eseguito correttamente.



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 l'API Astra"](#).



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. L'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.

Visualizzare snapshot e backup

È possibile visualizzare le istantanee e i backup di un'applicazione dalla scheda Data Protection (protezione dati).

Fasi

1. Fare clic su **Apps** (applicazioni), quindi sul nome di un'applicazione.
2. Fare clic su **Data Protection** (protezione dati).

Le istantanee vengono visualizzate per impostazione predefinita.

3. Fare clic su **Backup** per visualizzare l'elenco dei backup.

Eliminare le istantanee

Eliminare le snapshot pianificate o on-demand non più necessarie.

Fasi

1. Fare clic su **Apps** (applicazioni), quindi sul nome di un'applicazione.
2. Fare clic su **Data Protection** (protezione dati).
3. Fare clic sull'elenco a discesa nella colonna **Actions** per l'istananea desiderata.
4. Fare clic su **Delete snapshot** (Elimina snapshot).
5. Digitare la parola "DELETE" per confermare l'eliminazione, quindi fare clic su **Yes, Delete snapshot** (Sì, Elimina snapshot).

Risultato

Astra Control Center elimina lo snapshot.

Eliminare i backup

Eliminare i backup pianificati o on-demand non più necessari.



Non esiste alcun modo per interrompere un backup in esecuzione. Se è necessario eliminare il backup, attendere che sia stato completato, quindi seguire queste istruzioni. Per eliminare un backup non riuscito, ["Utilizzare l'API Astra"](#).

1. Fare clic su **Apps** (applicazioni), quindi sul nome di un'applicazione.
2. Fare clic su **Data Protection** (protezione dati).
3. Fare clic su **Backup**.
4. Fare clic sull'elenco a discesa nella colonna **Actions** per il backup desiderato.
5. Fare clic su **Delete backup** (Elimina backup).
6. Digitare la parola "DELETE" per confermare l'eliminazione, quindi fare clic su **Yes, Delete backup**.

Risultato

Astra Control Center elimina il backup.

Ripristinare le applicazioni

Astra Control Center può ripristinare l'applicazione da uno snapshot o da un backup. I backup e le snapshot persistenti dello storage vengono trasferiti dall'archivio a oggetti, pertanto il ripristino da uno snapshot esistente allo stesso cluster sarà più rapido rispetto ad altri metodi. È possibile utilizzare l'interfaccia utente Astra o ["L'API Astra"](#) per ripristinare le applicazioni.



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. Le app implementate con Helm 2 non sono supportate.



Se si esegue il ripristino in un cluster diverso, assicurarsi che il cluster utilizzi la stessa modalità di accesso al volume persistente (ad esempio ReadWriteMany). L'operazione di ripristino non riesce se la modalità di accesso al volume persistente di destinazione è diversa.



Quando crei un progetto per ospitare un'applicazione su un cluster OpenShift, al progetto (o namespace Kubernetes) viene assegnato un UID SecurityContext. Per consentire ad Astra Control Center di proteggere la tua applicazione e spostarla in un altro cluster o progetto in OpenShift, devi aggiungere policy che consentano all'applicazione di essere eseguita come qualsiasi UID. Ad esempio, i seguenti comandi CLI di OpenShift concedono le policy appropriate a un'applicazione WordPress.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

Fasi

1. Fare clic su **Apps** (applicazioni), quindi sul nome di un'applicazione.
2. Fare clic su **Data Protection**.
3. Se si desidera eseguire il ripristino da uno snapshot, tenere selezionata l'icona **Snapshot**. In caso contrario, fare clic sull'icona **Backup** per eseguire il ripristino da un backup.
4. Fare clic sull'elenco a discesa nella colonna **azioni** per lo snapshot o il backup da cui si desidera eseguire il ripristino.
5. Fare clic su **Ripristina applicazione**.
6. **Dettagli ripristino**: Specificare i dettagli per il ripristino:
 - Immettere un nome e uno spazio dei nomi per l'applicazione.



Se stai ripristinando un'applicazione che è stata eliminata, scegli un nome e uno spazio dei nomi diversi per l'applicazione rispetto al nome originale. Se il nome dell'applicazione ripristinata è uguale a quello dell'applicazione eliminata, l'operazione di ripristino non riesce.

- Scegliere il cluster di destinazione per l'applicazione.
 - Fare clic su **Review** (Rivedi).
7. **Restore Summary** (Riepilogo ripristino): Esaminare i dettagli relativi all'azione di ripristino e fare clic su **Restore** (Ripristina).

Risultato

Astra Control Center ripristina l'applicazione in base alle informazioni fornite.



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. L'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.

Clonare e migrare le applicazioni

Clonare un'applicazione esistente per creare un'applicazione duplicata sullo stesso cluster Kubernetes o su un altro cluster. La clonazione può essere di aiuto nel caso in cui sia necessario spostare applicazioni e storage da un cluster Kubernetes a un altro. Ad esempio, è possibile spostare i carichi di lavoro attraverso una pipeline ci/CD e attraverso gli spazi dei nomi Kubernetes. È possibile utilizzare l'interfaccia utente Astra o ["L'API Astra"](#) per clonare e migrare le applicazioni.



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

Quando Astra Control Center clona un'applicazione, crea un clone della configurazione dell'applicazione e dello storage persistente.



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.



Quando crei un progetto per ospitare un'applicazione su un cluster OpenShift, al progetto (o namespace Kubernetes) viene assegnato un UID SecurityContext. Per consentire ad Astra Control Center di proteggere la tua applicazione e spostarla in un altro cluster o progetto in OpenShift, devi aggiungere policy che consentano all'applicazione di essere eseguita come qualsiasi UID. Ad esempio, i seguenti comandi CLI di OpenShift concedono le policy appropriate a un'applicazione WordPress.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

Di cosa hai bisogno

Per clonare le applicazioni in un cluster diverso, è necessario un bucket predefinito. Quando si aggiunge il primo bucket, questo diventa quello predefinito.

Fasi

1. Fare clic su **Apps** (applicazioni).
2. Effettuare una delle seguenti operazioni:
 - Fare clic sull'elenco a discesa nella colonna **azioni** dell'applicazione desiderata.
 - Fare clic sul nome dell'applicazione desiderata e selezionare l'elenco a discesa Status (Stato) nella parte superiore destra della pagina.
3. Fare clic su **Clone**.
4. **Clone Details**: Specificare i dettagli per il clone:
 - Immettere un nome.
 - Immettere uno spazio dei nomi per il clone.
 - Scegliere un cluster di destinazione per il clone.

- Scegliere se si desidera creare il clone da uno snapshot o da un backup esistente. Se non si seleziona questa opzione, Astra Control Center crea il clone dallo stato corrente dell'applicazione.
5. **Origine:** Se si sceglie di clonare da uno snapshot o da un backup esistente, scegliere lo snapshot o il backup che si desidera utilizzare.
 6. Fare clic su **Review** (Rivedi).
 7. **Clone Summary:** Leggi i dettagli sul clone e fai clic su **Clone**.

Risultato

Astra Control Center clona l'applicazione in base alle informazioni fornite. L'operazione di clonazione viene eseguita correttamente quando il nuovo clone dell'applicazione si trova in *Available* nella pagina **Apps**.

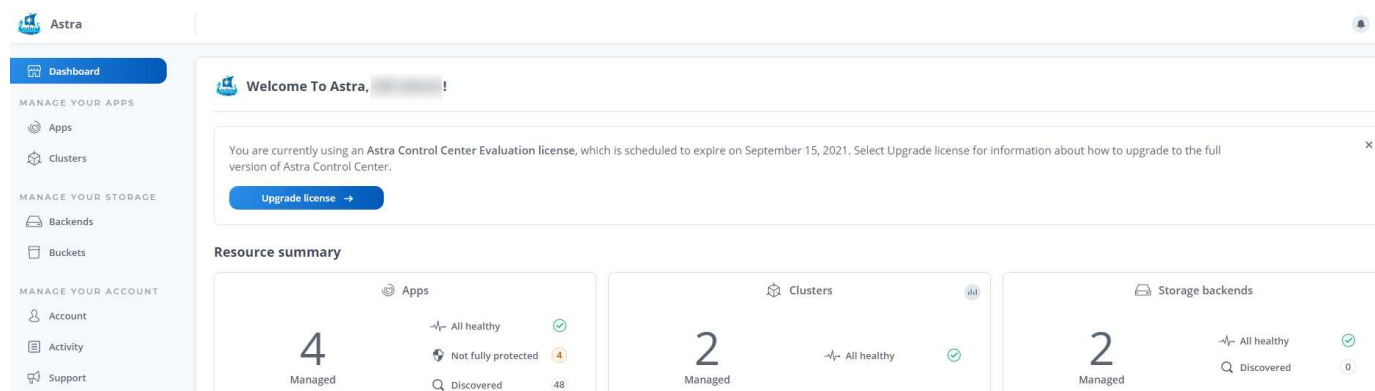


Dopo un'operazione di protezione dei dati (clone, backup, ripristino) e il successivo ridimensionamento persistente del volume, si verifica un ritardo di venti minuti prima che le nuove dimensioni del volume vengano visualizzate nell'interfaccia utente. L'operazione di protezione dei dati viene eseguita 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.

Visualizzare lo stato delle applicazioni e del cluster

Visualizza un riepilogo dello stato delle applicazioni e dei cluster

Seleziona la * dashboard* per visualizzare una vista di alto livello delle tue app, cluster, backend di storage e della loro salute.



Questi non sono solo numeri statici o stati, ma è possibile eseguire il drill-down da ciascuno di questi. Ad esempio, se le applicazioni non sono completamente protette, puoi passare il mouse sull'icona per identificare le applicazioni non completamente protette, il che include un motivo.

Riquadro Apps (applicazioni)

Il riquadro **Apps** consente di identificare quanto segue:

- Quante app stai attualmente gestendo con Astra.
- Se queste applicazioni gestite sono in buona salute.
- Se le applicazioni sono completamente protette (sono protette se sono disponibili backup recenti).
- Il numero di applicazioni rilevate, ma non ancora gestite.

Idealmente, questo numero sarebbe pari a zero perché, una volta scoperte, gestireste o ignorereste le applicazioni. Quindi, è necessario monitorare il numero di applicazioni rilevate nella dashboard per identificare quando gli sviluppatori aggiungono nuove applicazioni a un cluster.

Riquadro dei cluster

Il riquadro **Clusters** fornisce dettagli simili sullo stato dei cluster gestiti tramite Astra Control Center e consente di analizzare più dettagli come con un'applicazione.

Riquadro backend storage

Il riquadro **Storage backend** fornisce informazioni utili per identificare lo stato dei back-end dello storage, tra cui:

- Quanti backend di storage vengono gestiti
- Se questi backend gestiti sono in buono stato
- Se i backend sono completamente protetti
- Il numero di backend rilevati, ma non ancora gestiti.

Visualizza lo stato di salute e i dettagli dei cluster

Dopo aver aggiunto i cluster da gestire da Astra Control Center, è possibile visualizzare i dettagli del cluster, ad esempio la sua posizione, i nodi di lavoro, i volumi persistenti e le classi di storage.

Fasi

1. Nell'interfaccia utente di Astra Control Center, selezionare **Clusters**.
2. Nella pagina **Clusters**, selezionare il cluster di cui si desidera visualizzare i dettagli.
3. Visualizzare le informazioni nelle schede **Overview**, **Storage** e **Activity** per trovare le informazioni desiderate.
 - **Panoramica**: Dettagli sui nodi di lavoro, incluso il loro stato.
 - **Storage**: I volumi persistenti associati al calcolo, inclusi la classe e lo stato dello storage.
 - **Attività**: Mostra le attività correlate al cluster.



È inoltre possibile visualizzare le informazioni sul cluster partendo da Astra Control Center **Dashboard**. Nella scheda **Clusters** sotto **Riepilogo risorse**, è possibile selezionare i cluster gestiti, che consentono di accedere alla pagina **Clusters**. Una volta visualizzata la pagina **Clusters**, seguire la procedura descritta in precedenza.

Visualizza lo stato di salute e i dettagli di un'applicazione

Dopo aver iniziato a gestire un'applicazione, Astra fornisce informazioni dettagliate sull'applicazione che consentono di identificarne lo stato (se è integro), lo stato di protezione (se è completamente protetto in caso di guasto), i pod, lo storage persistente e molto altro ancora.

Fasi

1. Nell'interfaccia utente di Astra Control Center, selezionare **Apps**, quindi selezionare il nome di un'applicazione.
2. Fai clic per trovare le informazioni che cerchi:

Stato dell'app

Fornisce uno stato che riflette lo stato dell'applicazione in Kubernetes. Ad esempio, i pod e i volumi persistenti sono online? Se un'applicazione non è in buone condizioni, è necessario risolvere il problema sul cluster osservando i log di Kubernetes. Astra non fornisce informazioni utili per la risoluzione di un'applicazione guasta.

Stato di protezione dell'app

Fornisce uno stato di protezione dell'applicazione:

- **Completamente protetto:** L'applicazione dispone di una pianificazione di backup attiva e di un backup riuscito che risale a meno di una settimana fa
- **Protezione parziale:** L'applicazione dispone di una pianificazione di backup attiva, di una pianificazione di snapshot attiva o di un backup o snapshot riuscito
- **Non protetto:** Applicazioni non completamente protette o parzialmente protette.

Non è possibile essere completamente protetti fino a quando non si dispone di un backup recente. Ciò è importante perché i backup vengono memorizzati in un archivio a oggetti lontano dai volumi persistenti. Se un guasto o un incidente cancella il cluster e lo storage persistente, è necessario un backup per il ripristino. Un'istantanea non ti consentirebbe di ripristinarla.

Panoramica

Informazioni sullo stato dei pod associati all'applicazione.

Protezione dei dati

Consente di configurare una policy di protezione dei dati e di visualizzare le snapshot e i backup esistenti.

Storage

Mostra i volumi persistenti a livello di applicazione. Lo stato di un volume persistente è dal punto di vista del cluster Kubernetes.

Risorse

Consente di verificare quali risorse vengono sottoposte a backup e gestite.

Attività

Mostra le attività correlate all'applicazione.



È inoltre possibile visualizzare le informazioni dell'applicazione partendo da Astra Control Center **Dashboard**. Nella scheda **Apps** sotto **Resource summary**, è possibile selezionare le applicazioni gestite, che consentono di accedere alla pagina **Apps**. Una volta visualizzata la pagina **Apps**, seguire i passaggi descritti in precedenza.

Gestisci il tuo account

Gestire gli utenti

È possibile aggiungere, rimuovere e modificare gli utenti dell'installazione di Astra Control Center utilizzando l'interfaccia utente di Astra Control Center. È possibile utilizzare l'interfaccia utente Astra o ["L'API Astra"](#) per gestire gli utenti.

Aggiungere utenti

Gli account Owner e gli amministratori possono aggiungere altri utenti all'installazione di Astra Control Center.

Fasi

1. Nell'area di navigazione **Gestisci account**, fare clic su **account**.
2. Selezionare la scheda **utenti**.
3. Selezionare **Aggiungi utente**.
4. Immettere il nome dell'utente, l'indirizzo e-mail e una password temporanea.

L'utente dovrà modificare la password al primo accesso.

5. Selezionare un ruolo utente con le autorizzazioni di sistema appropriate.

Ciascun ruolo fornisce le seguenti autorizzazioni:

- Un **Viewer** può visualizzare le risorse.
- Un **Member** dispone delle autorizzazioni di ruolo Viewer e può gestire app e cluster, ma non può annullare la gestione di app o cluster o eliminare snapshot o backup.
- Un **Admin** dispone delle autorizzazioni di ruolo membro e può aggiungere e rimuovere qualsiasi altro utente ad eccezione del Proprietario.
- Un **Owner** dispone delle autorizzazioni di ruolo Admin e può aggiungere e rimuovere qualsiasi account utente.

6. Fare clic su **Aggiungi**.

Gestire le password

Puoi gestire le password per gli account utente in Astra Control Center.

Modificare la password

È possibile modificare la password dell'account utente in qualsiasi momento.

Fasi

1. Fare clic sull'icona User (utente) nella parte superiore destra della schermata.
2. Selezionare **Profilo**.
3. Fare clic sull'elenco a discesa **azioni** e selezionare **Modifica password**.
4. Immettere una password conforme ai requisiti.
5. Immettere nuovamente la password per confermare.
6. Fare clic su **Change password** (Modifica password).

Reimpostare la password di un altro utente

Se l'account dispone delle autorizzazioni di ruolo Amministratore o Proprietario, è possibile reimpostare le password per altri account utente e per i propri. Quando si reimposta una password, si assegna una password temporanea che l'utente dovrà modificare al momento dell'accesso.

Fasi

1. Nell'area di navigazione **Gestisci account**, fare clic su **account**.
2. Nella scheda **utenti**, selezionare l'elenco a discesa nella colonna **Stato** dell'utente.
3. Selezionare **Reset Password** (Ripristina password).
4. Immettere una password temporanea conforme ai requisiti della password.
5. Immettere nuovamente la password per confermare.



Al successivo accesso, all'utente verrà richiesto di modificare la password.

6. Fare clic su **Reset password** (Ripristina password).

Modificare il ruolo di un utente

Gli utenti con il ruolo Owner possono modificare il ruolo di tutti gli utenti, mentre gli utenti con il ruolo Admin possono modificare il ruolo degli utenti con il ruolo Admin, Member o Viewer.

Fasi

1. Nell'area di navigazione **Gestisci account**, fare clic su **account**.
2. Nella scheda **utenti**, selezionare l'elenco a discesa nella colonna **ruolo** dell'utente.
3. Selezionare un nuovo ruolo, quindi fare clic su **Cambia ruolo** quando richiesto.

Risultato

Astra Control Center aggiorna le autorizzazioni dell'utente in base al nuovo ruolo selezionato.

Rimuovere gli utenti

Gli utenti con il ruolo Owner (Proprietario) o Admin (Amministratore) possono rimuovere altri utenti dall'account in qualsiasi momento.

Fasi

1. Nell'area di navigazione **Gestisci account**, fare clic su **account**.
2. Nella scheda **utenti**, selezionare la casella di controllo nella riga di ciascun utente che si desidera rimuovere.
3. Fare clic su **azioni** e selezionare **Rimuovi utenti**.
4. Quando richiesto, confermare l'eliminazione digitando la parola "remove" (Rimuovi), quindi fare clic su **Yes, Remove User** (Sì, Rimuovi utente).

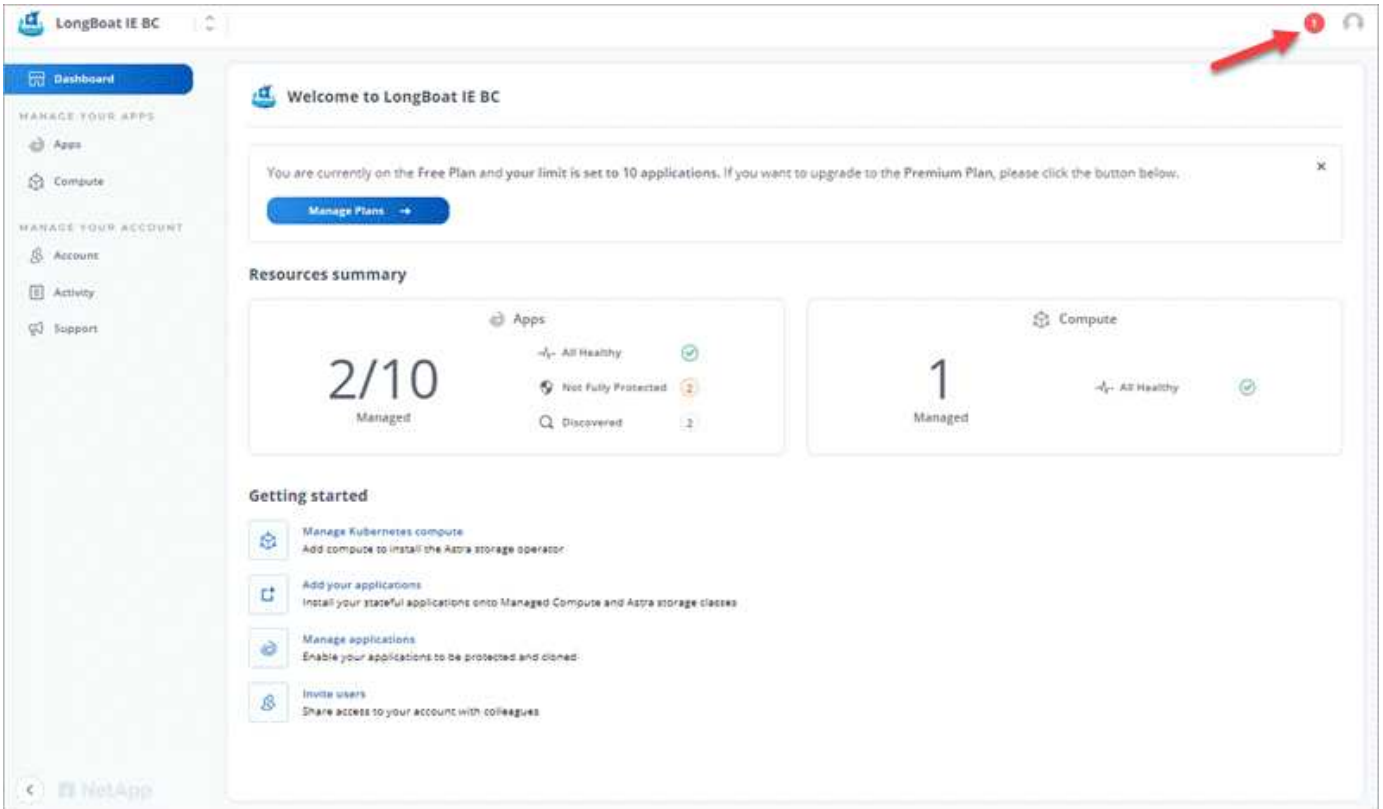
Risultato

Astra Control Center rimuove l'utente dall'account.

Visualizzare e gestire le notifiche

Astra informa l'utente quando le azioni sono state completate o non sono riuscite. Ad esempio, se il backup di un'applicazione è stato completato correttamente, viene visualizzata una notifica.

Il numero di notifiche non lette è disponibile nella parte superiore destra dell'interfaccia:



Puoi visualizzare queste notifiche e contrassegnarle come lette (questa operazione può risultare utile se desideri cancellare le notifiche non lette come noi).

Fasi

1. Fare clic sul numero di notifiche non lette in alto a destra.



2. Esaminare le notifiche, quindi fare clic su **Contrassegna come letto** o su **Mostra tutte le notifiche**.

Se si fa clic su **Mostra tutte le notifiche**, viene caricata la pagina Notifiche.

3. Nella pagina **Notifiche**, visualizzare le notifiche, selezionare quelle che si desidera contrassegnare come lette, fare clic su **azione** e selezionare **Contrassegna come letta**.

Aggiungere e rimuovere le credenziali

Aggiungi e rimuovi le credenziali per i provider di cloud privato locali, come ONTAP S3, i cluster Kubernetes gestiti con OpenShift o i cluster Kubernetes non gestiti dal tuo account in qualsiasi momento. Astra Control Center utilizza queste credenziali per scoprire i cluster Kubernetes e le applicazioni sui cluster e per eseguire il provisioning delle risorse per conto dell'utente.

Tutti gli utenti di Astra Control Center condividono gli stessi set di credenziali.

Aggiungere credenziali

È possibile aggiungere credenziali ad Astra Control Center quando si gestiscono i cluster. Per aggiungere credenziali aggiungendo un nuovo cluster, vedere ["Aggiungere un cluster Kubernetes"](#).



Se crei il tuo `kubeconfig` file, è necessario definire solo **un** elemento di contesto al suo interno. Vedere ["Documentazione Kubernetes"](#) per informazioni sulla creazione `kubeconfig` file.

Rimuovere le credenziali

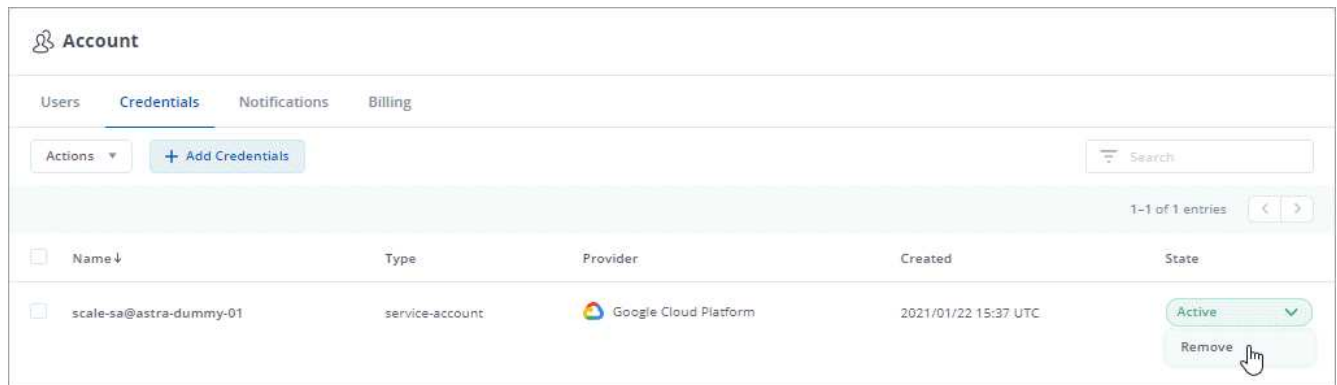
Rimuovere le credenziali da un account in qualsiasi momento. Rimuovere le credenziali solo dopo ["annullamento della gestione di tutti i cluster associati"](#).



Il primo set di credenziali aggiunto ad Astra Control Center è sempre in uso perché Astra Control Center utilizza le credenziali per l'autenticazione nel bucket di backup. Si consiglia di non rimuovere queste credenziali.

Fasi

1. Fare clic su **account > Credentials**.
2. Fare clic sull'elenco a discesa nella colonna **Stato** per le credenziali che si desidera rimuovere.
3. Fare clic su **Rimuovi**.



4. Digitare la parola "remove" per confermare l'eliminazione, quindi fare clic su **Yes, Remove Credential** (Sì, Rimuovi credenziale).

Risultato

Astra Control Center rimuove le credenziali dall'account.

Aggiornare una licenza esistente

È possibile convertire una licenza di valutazione in una licenza completa oppure aggiornare una licenza di valutazione o una licenza completa esistente con una nuova licenza. Se non si dispone di una licenza completa, rivolgersi al contatto commerciale NetApp per ottenere una licenza completa e un numero di serie. È possibile utilizzare l'interfaccia utente Astra o ["L'API Astra"](#) per aggiornare una licenza esistente.

Fasi

1. Accedere al sito di supporto NetApp.
2. Accedere alla pagina di download di Astra Control Center, inserire il numero di serie e scaricare il file di licenza NetApp completo (NLF).
3. Accedere all'interfaccia utente di Astra Control Center.
4. Dalla barra di navigazione a sinistra, selezionare **account > licenza**.
5. Nella pagina **account > licenza**, fare clic sul menu a discesa dello stato della licenza esistente e selezionare **Sostituisci**.
6. Individuare il file di licenza scaricato.
7. Selezionare **Aggiungi**.

La pagina **account > licenze** visualizza le informazioni sulla licenza, la data di scadenza, il numero di serie della licenza, l'ID account e le unità CPU utilizzate.

Gestire i bucket

Un provider di bucket dell'archivio di oggetti è essenziale se si desidera eseguire il backup delle applicazioni e dello storage persistente o se si desidera clonare le applicazioni tra cluster. Utilizzando Astra Control Center, Aggiungi un provider di archivi di oggetti come destinazione di backup off-cluster per le tue applicazioni.

Non è necessario un bucket se si clonano la configurazione dell'applicazione e lo storage persistente sullo stesso cluster.

Utilizzare uno dei seguenti provider di bucket:

- NetApp ONTAP S3
- NetApp StorageGRID S3
- Generico S3



Sebbene Astra Control Center supporti Amazon S3 come provider di bucket S3 generico, Astra Control Center potrebbe non supportare tutti i vendor di archivi di oggetti che sostengono il supporto S3 di Amazon.

Non è possibile eliminare un bucket, tuttavia è possibile modificarlo.

Un bucket può trovarsi in uno dei seguenti stati:

- In sospeso: Il bucket è pianificato per il rilevamento.
- Disponibile: La benna è disponibile per l'uso.
- Rimosso: Il bucket non è attualmente accessibile.

Per istruzioni su come gestire i bucket utilizzando l'API Astra, vedere ["Astra Automation e informazioni API"](#).

È possibile eseguire queste attività relative alla gestione dei bucket:

- ["Aggiungi un bucket"](#)
- ["Modificare un bucket"](#)



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.

Rimuovere le credenziali

Rimuovere le credenziali S3 da un account in qualsiasi momento utilizzando l'API Astra Control.

Per ulteriori informazioni, vedere ["Utilizzare l'API di controllo Astra"](#).



Il primo set di credenziali aggiunto ad Astra Control è sempre in uso perché Astra Control utilizza le credenziali per autenticare il bucket di backup. Si consiglia di non rimuovere queste credenziali.

Modificare un bucket

È possibile modificare le informazioni delle credenziali di accesso per un bucket e modificare se un bucket selezionato è il bucket predefinito.



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

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Bucket**.
2. Dal menu Actions (azioni), selezionare **Edit** (Modifica).
3. Modificare qualsiasi informazione diversa dal tipo di bucket.



Impossibile modificare il tipo di bucket.

4. Selezionare **Aggiorna**.

Trova ulteriori informazioni

- ["Utilizzare l'API Astra"](#)

Gestire il back-end dello storage

La gestione dei cluster di storage in Astra Control come back-end dello storage consente di ottenere collegamenti tra volumi persistenti (PVS) e il back-end dello storage, oltre a metriche di storage aggiuntive. È possibile monitorare la capacità dello storage e i dettagli relativi allo stato di salute, incluse le prestazioni, se il centro di controllo Astra è connesso a Cloud Insights.

Per istruzioni su come gestire i back-end dello storage utilizzando l'API Astra, vedere ["Astra Automation e informazioni API"](#).

È possibile completare le seguenti attività relative alla gestione di un backend di storage:

- ["Aggiungere un backend di storage"](#)
- [Visualizza i dettagli del back-end dello storage](#)
- [Annullare la gestione di un backend di storage](#)

Visualizza i dettagli del back-end dello storage

È possibile visualizzare le informazioni di back-end dello storage dalla dashboard o dall'opzione Backend.

Visualizza i dettagli del back-end dello storage dalla dashboard

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Dashboard**.
2. Esaminare la sezione Storage backend che mostra lo stato:
 - **Non integro:** Lo storage non è in uno stato ottimale. Ciò potrebbe essere dovuto a un problema di

latenza o a un'applicazione degradata, ad esempio, a causa di un problema di container.

- **Tutto sano:** Lo storage è stato gestito ed è in uno stato ottimale.
- **Scoperto:** Lo storage è stato scoperto, ma non gestito da Astra Control.

Visualizza i dettagli del back-end dello storage dall'opzione Backend

Visualizza informazioni sullo stato, la capacità e le performance del back-end (throughput IOPS e/o latenza).

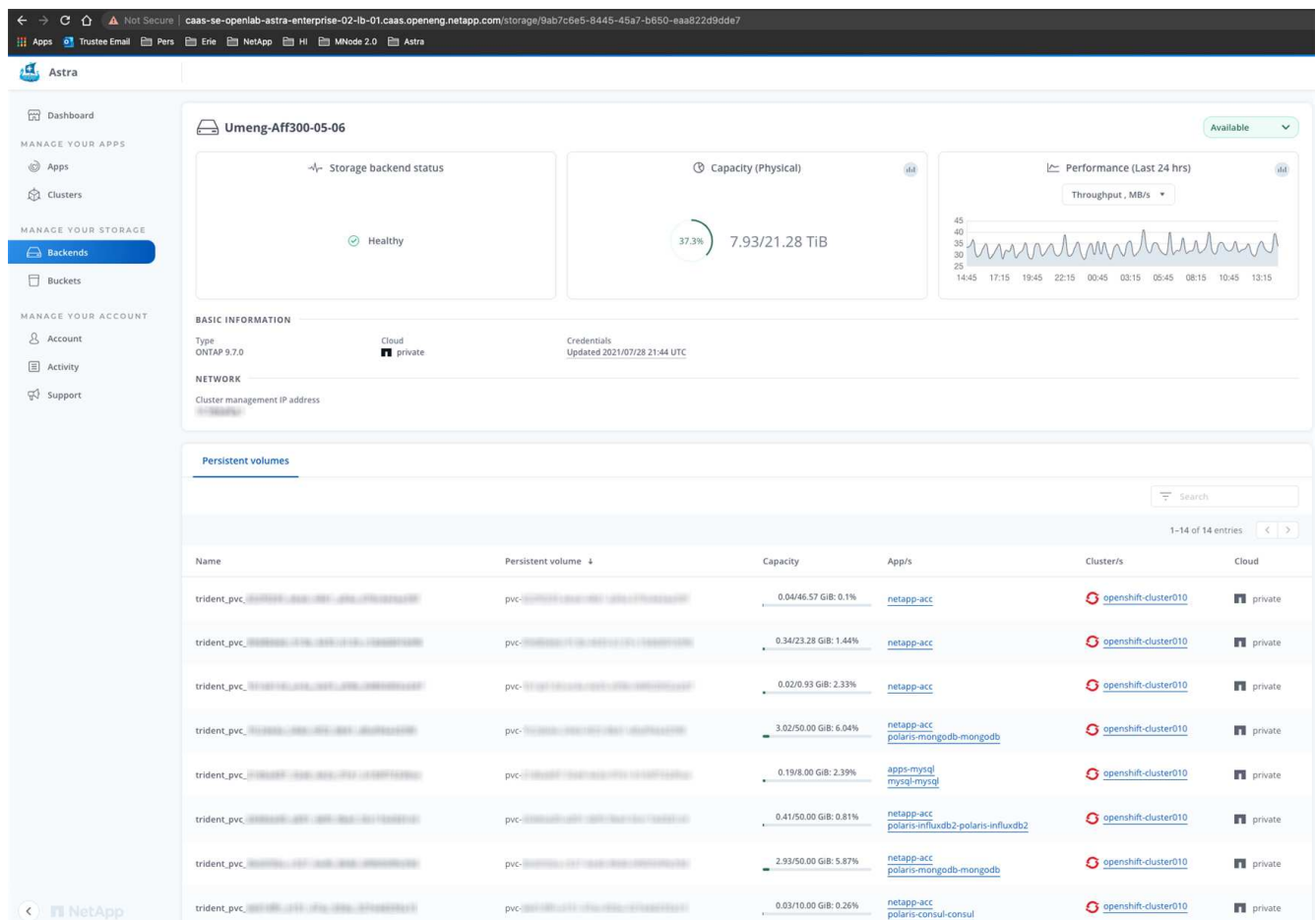
Con una connessione a Cloud Insights, è possibile visualizzare i volumi utilizzati dalle applicazioni Kubernetes, che vengono memorizzati in un backend di storage selezionato.

Fasi

1. Nell'area di navigazione a sinistra, selezionare **Backend**.
2. Selezionare il backend dello storage.



Se si è connessi a NetApp Cloud Insights, gli estratti di dati da Cloud Insights vengono visualizzati nella pagina backend.



3. Per accedere direttamente a Cloud Insights, fare clic sull'icona **Cloud Insights** accanto all'immagine delle metriche.

Annullare la gestione di un backend di storage

È possibile annullare la gestione del backend.

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Backend**.
2. Selezionare lo storage back-end.
3. Dal menu Actions (azioni), selezionare **UnManage** (Annulla gestione).
4. Digitare "unManage" per confermare la rimozione.
5. Selezionare **Sì, rimuovere il backend di storage**.

Trova ulteriori informazioni

- ["Utilizzare l'API Astra"](#)

Monitorare e proteggere l'infrastruttura

È possibile configurare diverse impostazioni opzionali per migliorare l'esperienza di Astra Control Center. Se la rete in cui si utilizza Astra Control Center richiede un proxy per la connessione a Internet (per caricare pacchetti di supporto sul sito di supporto NetApp o stabilire una connessione a Cloud Insights), è necessario configurare un server proxy in Astra Control Center. Per monitorare e ottenere informazioni sulla tua infrastruttura completa, crea una connessione con NetApp Cloud Insights. Per raccogliere gli eventi Kubernetes dai sistemi monitorati da Astra Control Center, aggiungere una connessione Fluentd.



Dopo aver attivato la connessione Cloud Insights, è possibile visualizzare le informazioni sul throughput nella pagina **backend** e connettersi a Cloud Insights da qui dopo aver selezionato un backend di storage. Le informazioni sono disponibili anche nella sezione cluster del pannello **Dashboard** e puoi collegarti a Cloud Insights da qui.

Aggiungere un server proxy

Se la rete in cui si utilizza Astra Control Center richiede un proxy per la connessione a Internet (per caricare pacchetti di supporto sul sito di supporto NetApp o stabilire una connessione a Cloud Insights), è necessario configurare un server proxy in Astra Control Center.



Astra Control Center non convalida i dati immessi per il server proxy. Assicurarsi di immettere i valori corretti.

Fasi

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin/owner**.
2. Selezionare **account > connessioni**.
3. Selezionare **Connect** dall'elenco a discesa per aggiungere un server proxy.



HTTP PROXY

Configure Astra Control to send traffic through a proxy server.

Disconnected

Connect

4. Immettere il nome del server proxy o l'indirizzo IP e il numero della porta proxy.
5. Se il server proxy richiede l'autenticazione, selezionare la casella di controllo e immettere il nome utente e

la password.

6. Selezionare **Connect**.

Risultato

Se le informazioni sul proxy inserite sono state salvate, la sezione **Proxy HTTP** della pagina **account > connessioni** indica che è connesso e visualizza il nome del server.



Connected



HTTP PROXY ?

Server: proxy.example.com:8888

Authentication: Enabled

Modificare le impostazioni del server proxy

È possibile modificare le impostazioni del server proxy.

Fasi

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin/owner**.
2. Selezionare **account > connessioni**.
3. Selezionare **Edit** (Modifica) dall'elenco a discesa per modificare la connessione.
4. Modificare i dettagli del server e le informazioni di autenticazione.
5. Selezionare **Salva**.

Disattiva la connessione al server proxy

È possibile disattivare la connessione al server proxy. Prima di disattivare l'opzione, viene visualizzato un avviso che potrebbe causare interruzioni ad altre connessioni.

Fasi

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin/owner**.
2. Selezionare **account > connessioni**.
3. Selezionare **Disconnect** dall'elenco a discesa per disattivare la connessione.
4. Nella finestra di dialogo visualizzata, confermare l'operazione.

Connettersi a Cloud Insights

Per monitorare e ottenere informazioni sulla tua infrastruttura completa, collega NetApp Cloud Insights con la tua istanza del centro di controllo Astra. Cloud Insights è incluso nella licenza di Astra Control Center.



Cloud Insights deve essere accessibile dalla rete utilizzata dal centro di controllo Astra o indirettamente tramite un server proxy.



Quando il centro di controllo Astra è collegato a Cloud Insights, viene creato un pod unità di acquisizione. Questo pod raccoglie i dati dai back-end di storage gestiti dal centro di controllo Astra e li invia a Cloud Insights. Questo pod richiede 8 GB di RAM e 2 core CPU.

Di cosa hai bisogno

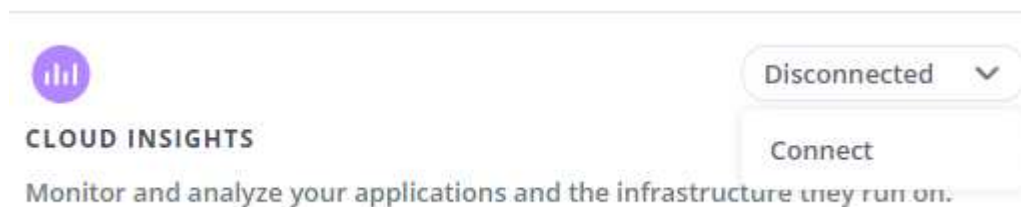
- Un account Astra Control Center con privilegi **admin/owner**.
- Una licenza Astra Control Center valida.
- Un server proxy se la rete in cui si utilizza Astra Control Center richiede un proxy per la connessione a Internet.



Se sei un nuovo utente di Cloud Insights, familiarizza con le caratteristiche e le funzionalità "qui".

Fasi

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin/owner**.
2. Selezionare **account > connessioni**.
3. Selezionare **Connect** dove nell'elenco a discesa viene visualizzato **disconnected** per aggiungere la connessione.



4. Inserire i token API Cloud Insights e l'URL del tenant. L'URL del tenant ha il seguente formato, ad esempio:

```
https://<environment-name>.c01.cloudinsights.netapp.com/
```

Quando si ottiene la licenza Cloud Insights, si ottiene l'URL del tenant. Se non si dispone dell'URL del tenant, consultare ["Documentazione Cloud Insights"](#).

- a. Per ottenere il **"Token API"**, Accedere all'URL del tenant Cloud Insights.
- b. In Cloud Insights, generare un token API di tipo **sola lettura**.

Name	Description	Token	API Type	Permission
astra_...		...zBskB1	All Categories	Read/Write
astra_...		...xKOel_	All Categories	Read/Write
astra_...		...2_A6HP	All Categories	Read Only
astra_...		...8BTKYY	All Categories	Read/Write

- c. Copiare la chiave **sola lettura**. Per attivare la connessione Cloud Insights, è necessario incollarla nella finestra di Astra Control Center.
- d. In Cloud Insights, generare un token API di tipo **lettura/scrittura**.
- e. Copiare la chiave **Read/Write**. È necessario incollarlo nella finestra di dialogo di Astra Control Center **Connect Cloud Insights**.



Si consiglia di generare una chiave **Read Only** e una chiave **Read/Write** e di non utilizzare la stessa chiave per entrambi gli scopi. Per impostazione predefinita, il periodo di scadenza del token è impostato su un anno. Si consiglia di mantenere la selezione predefinita per assegnare al token la durata massima prima della scadenza. Se il token scade, la telemetria si interrompe.

- f. Incollare le chiavi copiate da Cloud Insights in Astra Control Center.

5. Selezionare **Connect**.



Dopo aver selezionato **Connetti**, lo stato della connessione diventa **in sospeso** nella sezione **Cloud Insights** della pagina **account > connessioni**. L'attivazione della connessione e il passaggio allo stato **connesso** possono richiedere alcuni minuti.




Per passare facilmente da un'unità di controllo Astra a un'interfaccia utente Cloud Insights e viceversa, assicurarsi di aver effettuato l'accesso a entrambe.

Visualizzare i dati in Cloud Insights

Se la connessione ha avuto esito positivo, la sezione **Cloud Insights** della pagina **account > connessioni** indica che la connessione è stata stabilita e visualizza l'URL del tenant. È possibile visitare Cloud Insights per visualizzare e ricevere correttamente i dati.

EXTERNAL ?




HTTP PROXY ?

Server: [proxy.example.com:8888](#)

Authentication: Enabled

Connected



CLOUD INSIGHTS ?

Tenant: [Cloud Insights](#)

Connected

Se la connessione non è riuscita per qualche motivo, lo stato visualizza **Failed** (non riuscito). Il motivo del guasto è disponibile in **Notifiche** nella parte superiore destra dell'interfaccia utente.

Notifications

Mark All as Read

33



Unable to connect to Cloud Insights an hour ago

The Cloud Insights API token is invalid. Create a new API token in Cloud Insights and update Astra Control connection settings with the new token.

Le stesse informazioni sono disponibili anche in **account > Notifiche**.

Da Astra Control Center, è possibile visualizzare le informazioni sul throughput nella pagina **backend** e connettersi a Cloud Insights da qui dopo aver selezionato un backend di storage.

Backends

+ Manage

Search

★ Managed

Q Discovered

1-1 of 1 entries

Name	Status	Capacity	Throughput	Type	Actions
.06	✓	7.67/21.28 TiB: 36%	<div> <div>Throughput</div> <div>Last 24 hrs</div> <div> <div>5m ago: 8.00 MB/s</div> <div>Min: 4.00 MB/s</div> <div>Max: 11.00 MB/s</div> </div> <div>View in Cloud Insights</div> </div>	ONTAP 9.7.0	Available

Per accedere direttamente a Cloud Insights, selezionare l'icona **Cloud Insights** accanto all'immagine delle metriche.

Le informazioni sono disponibili anche nella *** Dashboard***.



Dopo aver attivato la connessione Cloud Insights, se si rimuovono i backend aggiunti in Centro di controllo Astra, i backend smettono di inviare i report a Cloud Insights.

Modificare la connessione Cloud Insights

È possibile modificare la connessione Cloud Insights.



È possibile modificare solo le chiavi API. Per modificare l'URL del tenant Cloud Insights, si consiglia di scollegare la connessione Cloud Insights e di connettersi al nuovo URL.

Fasi

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin/owner**.
2. Selezionare **account > connessioni**.
3. Selezionare **Edit** (Modifica) dall'elenco a discesa per modificare la connessione.
4. Modificare le impostazioni di connessione Cloud Insights.
5. Selezionare **Salva**.

Disattiva la connessione Cloud Insights

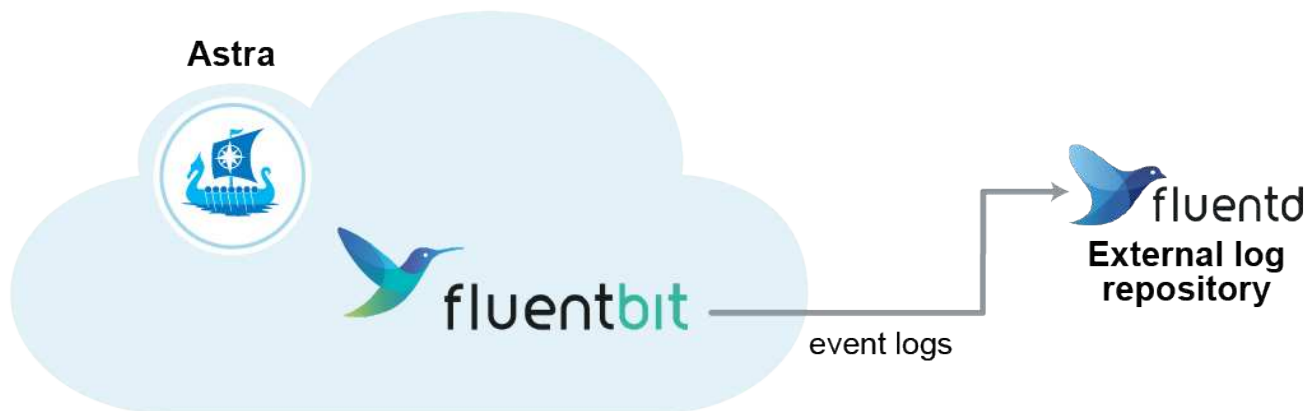
È possibile disattivare la connessione Cloud Insights per un cluster Kubernetes gestito da Astra Control Center. La disattivazione della connessione Cloud Insights non elimina i dati di telemetria già caricati su Cloud Insights.

Fasi

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin/owner**.
2. Selezionare **account > connessioni**.
3. Selezionare **Disconnect** dall'elenco a discesa per disattivare la connessione.
4. Nella finestra di dialogo visualizzata, confermare l'operazione. Dopo aver confermato l'operazione, nella pagina **account > connessioni**, lo stato Cloud Insights diventa **in sospeso**. Il passaggio allo stato **disconnesso** richiede alcuni minuti.

Connettersi a Fluentd

È possibile inviare registri (eventi Kubernetes) da Astra Control Center all'endpoint Fluentd. La connessione Fluentd è disattivata per impostazione predefinita.



A Fluentd vengono inoltrati solo i log degli eventi dei cluster gestiti.

Di cosa hai bisogno

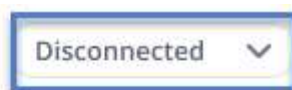
- Un account Astra Control Center con privilegi **admin/owner**.
- Astra Control Center installato e in esecuzione su un cluster Kubernetes.



Astra Control Center non convalida i dati immessi per il server Fluentd. Assicurarsi di immettere i valori corretti.

Fasi

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin/owner**.
2. Selezionare **account > connessioni**.
3. Selezionare **Connect** dall'elenco a discesa in cui viene visualizzato **disconnected** per aggiungere la connessione.



FLUENTD

Connect Astra Control logs to Fluentd for use by your log analysis software.

4. Inserire l'indirizzo IP dell'host, il numero di porta e la chiave condivisa per il server Fluentd.
5. Selezionare **Connect**.

Risultato

Se i dati immessi per il server Fluentd sono stati salvati, la sezione **Fluentd** della pagina **account > connessioni** indica che è connesso. A questo punto, è possibile visitare il server Fluentd collegato e visualizzare i registri degli eventi.

Se la connessione non è riuscita per qualche motivo, lo stato visualizza **Failed** (non riuscito). Il motivo del guasto è disponibile in **Notifiche** nella parte superiore destra dell'interfaccia utente.

Le stesse informazioni sono disponibili anche in **account > Notifiche**.



In caso di problemi con la raccolta dei log, è necessario accedere al nodo di lavoro e assicurarsi che i log siano disponibili in `/var/log/containers/`.

Modificare la connessione Fluentd

È possibile modificare la connessione di Fluentd all'istanza di Astra Control Center.

Fasi

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin/owner**.
2. Selezionare **account > connessioni**.
3. Selezionare **Edit** (Modifica) dall'elenco a discesa per modificare la connessione.
4. Modificare le impostazioni dell'endpoint Fluentd.
5. Selezionare **Salva**.

Disattiva la connessione Fluentd

È possibile disattivare la connessione di Fluentd all'istanza di Astra Control Center.

Fasi

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin/owner**.
2. Selezionare **account > connessioni**.
3. Selezionare **Disconnect** dall'elenco a discesa per disattivare la connessione.
4. Nella finestra di dialogo visualizzata, confermare l'operazione.

Aggiornare una licenza esistente

È possibile convertire una licenza di valutazione in una licenza completa oppure aggiornare una licenza di valutazione o una licenza completa esistente con una nuova licenza. Se non si dispone di una licenza completa, rivolgersi al contatto commerciale NetApp per ottenere una licenza completa e un numero di serie. È possibile utilizzare l'interfaccia utente Astra o ["L'API Astra"](#) per aggiornare una licenza esistente.

Fasi

1. Accedere al sito di supporto NetApp.
2. Accedere alla pagina di download di Astra Control Center, inserire il numero di serie e scaricare il file di licenza NetApp completo (NLF).
3. Accedere all'interfaccia utente di Astra Control Center.
4. Dalla barra di navigazione a sinistra, selezionare **account > licenza**.
5. Nella pagina **account > licenza**, fare clic sul menu a discesa dello stato della licenza esistente e selezionare **Sostituisci**.
6. Individuare il file di licenza scaricato.
7. Selezionare **Aggiungi**.

La pagina **account > licenze** visualizza le informazioni sulla licenza, la data di scadenza, il numero di serie della licenza, l'ID account e le unità CPU utilizzate.

Annulla la gestione di app e cluster

Rimuovi le app o i cluster che non vuoi più gestire da Astra Control Center.

Annullare la gestione di un'applicazione

Smetta di gestire le app che non vuoi più eseguire il backup, lo snapshot o la clonazione da Astra Control Center.

- Eventuali backup e snapshot esistenti verranno eliminati.
- Le applicazioni e i dati rimangono disponibili.

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Apps** (applicazioni).
2. Seleziona la casella di controllo delle applicazioni che non vuoi più gestire.
3. Dal menu **azione**, selezionare **Annulla gestione**.
4. Digitare "unManage" per confermare.
5. Confermare che si desidera annullare la gestione delle applicazioni, quindi selezionare **Sì, Annulla gestione applicazione**.

Risultato

Astra Control Center interrompe la gestione dell'applicazione.

Annullare la gestione di un cluster

Annulla la gestione del cluster che non si desidera più gestire da Astra Control Center.

- Questa azione impedisce la gestione del cluster da parte di Astra Control Center. Non apporta modifiche alla configurazione del cluster e non elimina il cluster.
- Trident non verrà disinstallato dal cluster. ["Scopri come disinstallare Trident"](#).



Prima di annullare la gestione del cluster, è necessario annullare la gestione delle applicazioni associate al cluster.

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Clusters**.
2. Selezionare la casella di controllo del cluster che non si desidera più gestire in Astra Control Center.
3. Dal menu **azioni**, selezionare **Annulla gestione**.
4. Confermare che si desidera annullare la gestione del cluster, quindi selezionare **Sì, Annulla gestione cluster**.

Risultato

Lo stato del cluster cambia in **Removing** (Rimozione), quindi il cluster viene rimosso dalla pagina **Clusters** e non viene più gestito da Astra Control Center.



Se il centro di controllo Astra e Cloud Insights non sono connessi, la disinstallazione del cluster rimuove tutte le risorse installate per l'invio dei dati di telemetria. **Se il centro di controllo Astra e Cloud Insights sono connessi**, la mancata gestione del cluster elimina solo il fluentbit e. event-exporter pod.

Disinstallare Astra Control Center

Potrebbe essere necessario rimuovere i componenti di Astra Control Center se si esegue l'aggiornamento da una versione di prova a una versione completa del prodotto. Per rimuovere Astra Control Center e Astra Control Center Operator, eseguire i comandi descritti in questa procedura in sequenza.

Di cosa hai bisogno

- Utilizzare l'interfaccia utente di Astra Control Center per annullare la gestione di tutto "cluster".

Fasi

1. Eliminare Astra Control Center. Il seguente comando di esempio si basa su un'installazione predefinita. Modificare il comando se sono state create configurazioni personalizzate.

```
kubectl delete -f astra_control_center_min.yaml -n netapp-acc
```

Risultato:

```
astracontrolcenter.astra.netapp.io "astra" deleted
```

2. Utilizzare il seguente comando per eliminare netapp-acc spazio dei nomi:

```
kubectl delete ns netapp-acc
```

Risultato:

```
namespace "netapp-acc" deleted
```

3. Utilizzare il seguente comando per eliminare i componenti del sistema dell'operatore di Astra Control Center:

```
kubectl delete -f astra_control_center_operator_deploy.yaml
```

Risultato:

```
namespace "netapp-acc-operator" deleted
customresourcedefinition.apiextensions.k8s.io
"astracontrolcenters.astra.netapp.io" deleted
role.rbac.authorization.k8s.io "acc-operator-leader-election-role"
deleted
clusterrole.rbac.authorization.k8s.io "acc-operator-manager-role"
deleted
clusterrole.rbac.authorization.k8s.io "acc-operator-metrics-reader"
deleted
clusterrole.rbac.authorization.k8s.io "acc-operator-proxy-role" deleted
rolebinding.rbac.authorization.k8s.io "acc-operator-leader-election-
rolebinding" deleted
clusterrolebinding.rbac.authorization.k8s.io "acc-operator-manager-
rolebinding" deleted
clusterrolebinding.rbac.authorization.k8s.io "acc-operator-proxy-
rolebinding" deleted
configmap "acc-operator-manager-config" deleted
service "acc-operator-controller-manager-metrics-service" deleted
deployment.apps "acc-operator-controller-manager" deleted
```

Trova ulteriori informazioni

- ["Problemi noti per la disinstallazione"](#)

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.