Documentazione di Astra Control Center 23,10

Astra Control Center

NetApp
August 11, 2025

Sommario

Documentazione di Astra Control Center 23,10 . . . 1
Note di rilascio . . . 2
Novità di questa release di Astra Control Center . . . 2
7 novembre 2023 (23.10.0) . . . 2
31 luglio 2023 (23.07.0) . . . 3
18 maggio 2023 (23.04.2) . . . 3
25 aprile 2023 (23.04.0) . . . 4
22 novembre 2022 (22.11.0) . . . 4
8 settembre 2022 (22.08.1) . . . 4
10 agosto 2022 (22.08.0) . . . 4
26 aprile 2022 (22.04.0) . . . 5
14 dicembre 2021 (21.12) . . . 5
5 agosto 2021 (21.08) . . . 6
Trova ulteriori informazioni . . . 6
Problemi noti . . . 6
I backup e le snapshot delle applicazioni non vengono eseguiti se la classe volumesnapshotclass viene aggiunta dopo la gestione di un cluster . . . 7
La gestione di un cluster con Astra Control Center non riesce quando il file kubeconfig contiene più di un contesto . . . 7
Un pod di monitoraggio può bloccarsi negli ambienti Istio . . . 7
Le operazioni di gestione dei dati dell'app non riescono e si verificano errori di servizio interni (500) quando Astra Trident è offline . . . 8
Le operazioni di ripristino in-place alle classi di storage economiche ontap-nas falliscono . . . 8
Il ripristino da un backup quando si utilizza la crittografia in-flight Kerberos può non riuscire . . . 8
I dati di backup rimangono nel bucket dopo l'eliminazione per bucket con criteri di conservazione scaduti . . . 8
Trova ulteriori informazioni . . . 9
Limitazioni note . . . 9
Lo stesso cluster non può essere gestito da due istanze di Astra Control Center . . . 9
Astra Control Center non è in grado di gestire due cluster con lo stesso nome . . . 10
Un utente con vincoli RBAC dello spazio dei nomi può aggiungere e annullare la gestione di un cluster . . . 11
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 . . . 11
Non è possibile ripristinare collettivamente più applicazioni in un singolo namespace in un namespace diverso . . . 11
Astra Control non supporta applicazioni che utilizzano più classi di storage per spazio dei nomi . . . 11
Astra Control non assegna automaticamente i bucket predefiniti per le istanze cloud . . . 11
I cloni delle applicazioni installate utilizzando operatori pass-by-reference possono fallire . . . 11
Le operazioni di ripristino in-place delle applicazioni che utilizzano un gestore dei certificati non sono supportate . . . 12
Le applicazioni implementate dall'operatore CON ambito cluster e abilitato OLM non sono supportate . . . 12
Le app implementate con Helm 2 non sono supportate . . . 12

Gli snapshot potrebbero non funzionare per i cluster Kubernetes 1.25 o versioni successive con determinate versioni di snapshot controller . . . 12
I backup e le snapshot potrebbero non essere conservati durante la rimozione di un'istanza di Astra Control Center . . . 12
Limitazioni di utenti e gruppi LDAP . . . 13
I bucket S3 in Astra Control Center non riportano la capacità disponibile . . . 13
Astra Control Center non convalida i dati immessi per il server proxy . . . 13
Le connessioni esistenti a un pod Postgres causano errori . . . 13
La pagina Activity (attività) visualizza fino a 100000 eventi . . . 13
SnapMirror non supporta le applicazioni che utilizzano NVMe su TCP per backend di storage . . . 13
Trova ulteriori informazioni . . . 13
Inizia subito . . . 14
Scopri di più su Astra Control . . . 14
Caratteristiche . . . 14
Modelli di implementazione . . . 14
Come funziona Astra Control Service . . . 15
Come funziona Astra Control Center . . . 16
Per ulteriori informazioni . . . 17
Requisiti di Astra Control Center . . . 17
Ambienti Kubernetes cluster host supportati . . . 17
Requisiti delle risorse del cluster host . . . 18
Requisiti mesh di servizio . . . 18
Requisiti di Astra Trident . . . 19
Astra Control provisioner . . . 19
Back-end dello storage . . . 19
Registro delle immagini . . . 20
Licenza Astra Control Center . . . 20
Requisiti di rete . . . 20
Ingresso per cluster Kubernetes on-premise . . . 22
Browser Web supportati . . . 22
Requisiti aggiuntivi per i cluster di applicazioni . . . 22
Cosa succederà . . . 22
Avvio rapido per Astra Control Center . . . 23
Per ulteriori informazioni . . . 24
Panoramica dell'installazione . . . 24
Installare Astra Control Center utilizzando il processo standard . . . 24
Installare Astra Control Center utilizzando OpenShift OperatorHub . . . 65
Installare il centro di controllo Astra con un backend di storage Cloud Volumes ONTAP . . . 75
Configurare Astra Control Center dopo l'installazione . . . 91
Configurare Astra Control Center . . . 97
Aggiungere una licenza per Astra Control Center . . . 97
Prepara il tuo ambiente per la gestione dei cluster utilizzando Astra Control . . . 98
Aggiungere il cluster . . . 109
Abilitare l'autenticazione sul backend dello storage ONTAP . . . 110
Aggiungere un backend di storage . . . 117

Aggiungi un bucket . . . 118
Quali sono le prossime novità? . . . 119
Domande frequenti per Astra Control Center . . . 120
Panoramica . . . 120
Accesso al centro di controllo Astra . . . 120
Licensing . . . 120
Registrazione dei cluster Kubernetes . . . 121
Gestione delle applicazioni . . . 121
Operazioni di gestione dei dati . . . 122
Astra Control provisioner . . . 122
Concetti . . . 125
Architettura e componenti . . . 125
Componenti di controllo Astra . . . 125
Interfacce di controllo Astra . . . 126
Per ulteriori informazioni . . . 126
Protezione dei dati . . . 126
Snapshot, backup e policy di protezione . . . 126
Cloni . . . 127
Replica tra back-end dello storage . . . 128
Backup, snapshot e cloni con una licenza scaduta . . . 130
Licensing . . . 130
Licenze di valutazione e licenze complete . . . 131
Scadenza della licenza . . . 131
Come viene calcolato il consumo delle licenze . . . 131
Trova ulteriori informazioni . . . 131
Gestione delle applicazioni . . . 131
Classi di storage e dimensioni del volume persistente . . . 134
Panoramica . . . 134
Classi di storage . . . 134
Per ulteriori informazioni . . . 134
Ruoli e spazi dei nomi degli utenti . . . 134
Ruoli utente . . . 134
Spazi dei nomi . . . 135
Trova ulteriori informazioni . . . 135
Utilizzare Astra Control Center . . . 136
Inizia a gestire le app . . . 136
Requisiti di gestione delle applicazioni . . . 136
Metodi di installazione delle applicazioni supportati . . . 136
Installa le app sul tuo cluster . . . 137
Definire le applicazioni . . . 137
E gli spazi dei nomi di sistema? . . . 141
Esempio: Policy di protezione separata per release diverse . . . 141
Trova ulteriori informazioni . . . 141
Proteggi le app . . . 141
Panoramica della protezione . . . 142

Proteggi le app con snapshot e backup . . . 142
Ripristinare le applicazioni . . . 150
Replica delle applicazioni tra back-end di storage utilizzando la tecnologia SnapMirror . . . 155
Clonare e migrare le applicazioni . . . 162
Gestire gli hook di esecuzione delle applicazioni . . . 165
Proteggi Astra Control Center con Astra Control Center . . . 174
Monitorare lo stato delle applicazioni e del cluster . . . 184
Visualizza un riepilogo dello stato delle applicazioni e dei cluster . . . 184
Visualizzare lo stato dei cluster e gestire le classi di storage . . . 185
Visualizza lo stato di salute e i dettagli di un'applicazione . . . 186
Gestisci il tuo account . . . 187
Gestire utenti e ruoli locali . . . 187
Gestire l'autenticazione remota . . . 190
Gestire utenti e gruppi remoti . . . 192
Visualizzare e gestire le notifiche . . . 194
Aggiungere e rimuovere le credenziali . . . 195
Monitorare l'attività dell'account . . . 195
Aggiornare una licenza esistente . . . 196
Gestire i bucket . . . 197
Modificare un bucket . . . 198
Impostare il bucket predefinito . . . 198
Ruotare o rimuovere le credenziali bucket . . . 198
Rimuovere una benna . . . 199
Trova ulteriori informazioni . . . 200
Gestire il back-end dello storage . . . 200
Visualizza i dettagli del back-end dello storage . . . 200
Modificare i dettagli dell'autenticazione back-end dello storage . . . 201
Gestire un backend di storage rilevato . . . 202
Annullare la gestione di un backend di storage . . . 202
Rimuovere un backend di storage . . . 203
Trova ulteriori informazioni . . . 203
Monitorare le attività in esecuzione . . . 203
Monitorare l'infrastruttura con connessioni Cloud Insights, Prometheus o Fluentd . . . 204
Aggiungere un server proxy per le connessioni a Cloud Insights o al sito di supporto NetApp . . . 204
Connettersi a Cloud Insights . . . 206
Connettiti a Prometheus . . . 209
Connettersi a Fluentd . . . 211
Annulla la gestione di app e cluster . . . 213
Annullare la gestione di un'applicazione . . . 213
Annullare la gestione di un cluster . . . 213
Aggiornare Astra Control Center . . . 214
Scarica ed estrai Astra Control Center . . . 216
Rimuovere il plug-in NetApp Astra kubectl e installarlo di nuovo . . . 217
Aggiungere le immagini al registro locale . . . 218
Installare l'operatore Astra Control Center aggiornato . . . 220

Aggiornare Astra Control Center . . . 224
Verificare lo stato del sistema . . . 226
Abilita Astra Control Provisioner . . . 226
(Fase 1) scaricare ed estrarre Astra Control Provisioner . . . 227
(Fase 2) attiva Astra Control Provisioner in Astra Trident . . . 230
Risultato . . . 233
Disinstallare Astra Control Center . . . 234
Risoluzione dei problemi di disinstallazione . . . 235
Trova ulteriori informazioni . . . 237
Utilizza Astra Control Provisioner . . . 238
Configurare la crittografia backend dello storage . . . 238
Configura la crittografia Kerberos in-flight con i volumi ONTAP in sede . . . 238
Configurare la crittografia Kerberos in-flight con i volumi Azure NetApp Files . . . 242
Ripristina i dati dei volumi utilizzando uno snapshot . . . 245
Replica dei volumi con SnapMirror . . . 247
Prerequisiti per la replica . . . 248
Creare un PVC specchiato . . . 248
Stati di replica dei volumi . . . 251
Promozione del PVC secondario durante un failover non pianificato . . . 251
Promozione del PVC secondario durante un failover pianificato . . . 252
Ripristinare una relazione di mirroring dopo un failover . . . 252
Operazioni supplementari . . . 252
Aggiorna relazioni mirror quando ONTAP è online . . . 253
Aggiorna relazioni di mirroring quando ONTAP non è in linea . . . 253
Automatizza con l'API REST di Astra Control . . . 254
Automazione mediante l'API REST di Astra Control . . . 254
Conoscenza e supporto . . . 255
Risoluzione dei problemi . . . 255
Richiedi assistenza . . . 255
Opzioni di supporto automatico . . . 255
Abilita il caricamento giornaliero del bundle di supporto pianificato sul supporto NetApp . . . 256
Generare bundle di supporto da fornire al supporto NetApp . . . 256
Versioni precedenti della documentazione di Astra Control Center . . . 258
Note legali . . . 259
Copyright . . . 259
Marchi . . . 259
Brevetti . . . 259
Direttiva sulla privacy . . . 259
Open source . . . 259
Licenza API Astra Control . . . 259

Documentazione di Astra Control Center 23,10

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.

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 volumi Azure NetApp Files e 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)

Dettagli

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)

Dettagli

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)

Dettagli

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)

Dettagli

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)

Dettagli

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)

Dettagli

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)

Dettagli

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)

Dettagli

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)

Dettagli

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
- Un pod di monitoraggio può bloccarsi negli ambienti Istio
- Le operazioni di gestione dei dati dell'app non riescono e si verificano errori di servizio interni (500) quando Astra Trident è offline
- Le operazioni di ripristino in-place alle classi di storage economiche ontap-nas falliscono
- 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.

Un pod di monitoraggio può bloccarsi negli ambienti Istio

Se si associa il centro di controllo Astra a Cloud Insights in un ambiente Istio, il `telegraf-rs` pod può bloccarsi. Per risolvere il problema, attenersi alla seguente procedura:

1. Individuare il pod bloccato:

   ```
   kubectl -n netapp-monitoring get pod | grep Error
   ```

   L'output dovrebbe essere simile a quanto segue:

   ```
   NAME READY STATUS RESTARTS AGE
   telegraf-rs-fhhrh 1/2 Error 2 (26s ago) 32s
   ```

2. Riavviare il pod bloccato, sostituendo `<pod_name_from_output>` con il nome del pod interessato:

   ```
   kubectl -n netapp-monitoring delete pod <pod_name_from_output>
   ```

   L'output dovrebbe essere simile a quanto segue:

```
pod "telegraf-rs-fhhrh" deleted
```

3. Verificare che il pod sia stato riavviato e che non si trovi in uno stato di errore:

```
kubectl -n netapp-monitoring get pod
```

L'output dovrebbe essere simile a quanto segue:

```
NAME READY STATUS RESTARTS AGE
telegraf-rs-rrnsb 2/2 Running 0 11s
```

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.

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.

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

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

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.

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.

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"

Inizia subito

Scopri di più su Astra Control

Astra Control è una soluzione per la gestione del ciclo di vita dei dati delle applicazioni Kubernetes che semplifica le operazioni per le applicazioni stateful. Proteggi, esegui il backup, replica e migra facilmente i carichi di lavoro Kubernetes e crea istantaneamente cloni applicativi funzionanti.

Caratteristiche

Astra Control offre funzionalità critiche per la gestione del ciclo di vita dei dati delle applicazioni Kubernetes:

- Gestire automaticamente lo storage persistente
- Creazione di snapshot e backup on-demand basati sulle applicazioni
- Automatizzare le operazioni di backup e snapshot basate su policy
- Migrare applicazioni e dati da un cluster Kubernetes a un altro
- Replica delle applicazioni su un sistema remoto utilizzando la tecnologia NetApp SnapMirror (Astra Control Center)
- Clonare le applicazioni dallo staging alla produzione
- Visualizzare lo stato di salute e protezione dell'applicazione
- Utilizzare un'interfaccia utente Web o un'API per implementare i flussi di lavoro di backup e migrazione

Modelli di implementazione

Astra Control è disponibile in due modelli di implementazione:

- **Astra Control Service**: Un servizio gestito da NetApp che offre la gestione dei dati application-aware dei cluster Kubernetes in ambienti di cloud provider multipli, oltre ai cluster Kubernetes autogestiti.
- **Astra Control Center**: Software autogestito che fornisce la gestione dei dati applicativa dei cluster Kubernetes in esecuzione nel tuo ambiente on-premise. Il centro di controllo Astra può essere installato anche in ambienti di cloud provider multipli con un backend di storage NetApp Cloud Volumes ONTAP.

	Servizio di controllo Astra	**Centro di controllo Astra**
Come viene offerto?	Come servizio cloud completamente gestito da NetApp	Come software che puoi scaricare, installare e gestire
Dove è ospitato?	Su un cloud pubblico scelto da NetApp	Sul tuo cluster Kubernetes
Come viene aggiornato?	Gestito da NetApp	Gli aggiornamenti vengono gestiti

	Servizio di controllo Astra	Centro di controllo Astra
Quali sono i backend di storage supportati?	• Servizi Web Amazon: ◦ Amazon EBS ◦ Amazon FSX per NetApp ONTAP ◦ "Cloud Volumes ONTAP" • Google Cloud: ◦ Disco persistente di Google ◦ NetApp Cloud Volumes Service ◦ "Cloud Volumes ONTAP" • Microsoft Azure: ◦ Dischi gestiti Azure ◦ Azure NetApp Files ◦ "Cloud Volumes ONTAP" • Cluster a gestione automatica: ◦ Amazon EBS ◦ Dischi gestiti Azure ◦ Disco persistente di Google ◦ "Cloud Volumes ONTAP" ◦ NetApp MetroCluster ◦ "Longhorn" • Cluster on-premise: ◦ NetApp MetroCluster ◦ Sistemi NetApp ONTAP AFF e FAS ◦ NetApp ONTAP Select ◦ "Cloud Volumes ONTAP" ◦ "Longhorn"	• Sistemi NetApp ONTAP AFF e FAS • NetApp ONTAP Select • "Cloud Volumes ONTAP"

Come funziona Astra Control Service

Astra Control Service è un servizio cloud gestito da NetApp sempre attivo e aggiornato con le funzionalità più recenti. Utilizza diversi componenti per consentire la gestione del ciclo di vita dei dati delle applicazioni.

Ad alto livello, Astra Control Service funziona come segue:

- Per iniziare a utilizzare Astra Control Service, devi configurare il tuo cloud provider e registrarti per un account Astra.
  - Per i cluster GKE, Astra Control Service utilizza "NetApp Cloud Volumes Service per Google Cloud" O Google Persistent Disks come back-end di storage per i volumi persistenti.
  - Per i cluster AKS, Astra Control Service utilizza "Azure NetApp Files" O Azure Managed Disks come

back-end di storage per i volumi persistenti.

    - Per i cluster Amazon EKS, Astra Control Service utilizza "Amazon Elastic Block Store" oppure "Amazon FSX per NetApp ONTAP" come back-end di storage per i volumi persistenti.

- Aggiungi il tuo primo calcolo Kubernetes ad Astra Control Service. Astra Control Service esegue le seguenti operazioni:
    - Crea un archivio di oggetti nel tuo account cloud provider, dove vengono memorizzate le copie di backup.

      In Azure, Astra Control Service crea anche un gruppo di risorse, un account di storage e chiavi per il container Blob.

    - Crea un nuovo ruolo di amministratore e un nuovo account del servizio Kubernetes sul cluster.
    - Utilizza il nuovo ruolo di amministratore per l'installazione "Astra Trident" sul cluster e per creare una o più classi di storage.
    - Se utilizzi un'offerta di cloud service storage NetApp come back-end dello storage, Astra Control Service utilizza Astra Trident per eseguire il provisioning di volumi persistenti per le tue applicazioni. Se si utilizzano dischi gestiti Amazon EBS o Azure come back-end dello storage, è necessario installare un driver CSI specifico del provider. Le istruzioni di installazione sono fornite in "Configurare Amazon Web Services" e. "Configurare Microsoft Azure con dischi gestiti Azure".
- A questo punto, è possibile aggiungere applicazioni al cluster. Il provisioning dei volumi persistenti verrà eseguito sulla nuova classe di storage predefinita.
- Quindi, utilizza Astra Control Service per gestire queste applicazioni e iniziare a creare snapshot, backup e cloni.

Il piano gratuito di Astra Control ti consente di gestire fino a 10 spazi dei nomi nel tuo account. Se desideri gestire più di 10, dovrai impostare la fatturazione eseguendo l'aggiornamento dal piano gratuito al piano Premium.

Come funziona Astra Control Center

Astra Control Center viene eseguito localmente nel tuo cloud privato.

Il centro di controllo Astra supporta i cluster Kubernetes con classe di storage basata su Astra Trident con un backend di storage ONTAP 9.5 e superiore.

In un ambiente connesso al cloud, Astra Control Center utilizza Cloud Insights per fornire monitoraggio e telemetria avanzati. In assenza di una connessione Cloud Insights, il monitoraggio e la telemetria sono disponibili in un centro di controllo Astra per un periodo di 7 giorni ed esportati anche in strumenti di monitoraggio nativi Kubernetes (come Prometheus e Grafana) attraverso endpoint di metriche aperte.

Astra Control Center è completamente integrato nell'ecosistema di consulente digitale di AutoSupport e Active IQ (detto anche Digital Advisor) per fornire agli utenti e al supporto NetApp informazioni su risoluzione dei problemi e utilizzo.

Puoi provare Astra Control Center utilizzando una licenza di valutazione integrata della durata di 90 giorni. Mentre stai valutando Astra Control Center, puoi ottenere supporto tramite e-mail e opzioni della community. Inoltre, puoi accedere agli articoli e alla documentazione della Knowledge base dalla dashboard di supporto all'interno del prodotto.

Per installare e utilizzare Astra Control Center, è necessario soddisfare determinati requisiti "requisiti".

Ad alto livello, Astra Control Center funziona come segue:

- Astra Control Center viene installato nel proprio ambiente locale. Scopri di più su come "Installare Astra Control Center".
- È possibile completare alcune attività di configurazione, come ad esempio:
  - Impostare la licenza.
  - Aggiungere il primo cluster.
  - Aggiungere il backend di storage rilevato quando si aggiunge il cluster.
  - Aggiungi un bucket di store di oggetti che memorizzerà i backup delle tue app.

Scopri di più su come "Configurare Astra Control Center".

È possibile aggiungere applicazioni al cluster. In alternativa, se nel cluster gestito sono già presenti alcune applicazioni, è possibile utilizzare Astra Control Center per gestirle. Quindi, utilizza Astra Control Center per creare snapshot, backup, cloni e relazioni di replica.

Per ulteriori informazioni

- "Documentazione del servizio Astra Control"
- "Documentazione di Astra Control Center"
- "Documentazione di Astra Trident"
- "Documentazione sull'API Astra Control"
- "Documentazione Cloud Insights"
- "Documentazione ONTAP"

Requisiti di Astra Control Center

Inizia verificando la preparazione del tuo ambiente operativo, dei cluster di applicazioni, delle applicazioni, delle licenze e del browser Web. Assicurati che il tuo ambiente soddisfi questi requisiti per implementare e utilizzare Astra Control Center.

Ambienti Kubernetes cluster host supportati

Astra Control Center è stato validato con i seguenti ambienti host Kubernetes:

> Assicurarsi che l'ambiente Kubernetes scelto per ospitare Astra Control Center soddisfi i requisiti di base delle risorse descritti nella documentazione ufficiale dell'ambiente.

Distribuzione di Kubernetes sul cluster host	Versioni supportate
Azure Kubernetes Service su Azure Stack HCI	Azure Stack HCI 21H2 e 22H2 con AKS 1.24.x e 1.25.x.
Google anthos	Da 1,15 a 1,16 (vedere Requisiti di ingresso di Google anthos)
Kubernetes (upstream)	da 1,26 a 1,28

Distribuzione di Kubernetes sul cluster host	Versioni supportate
Rancher Kubernetes Engine (RKE)	RKE 1.3 con Rancher Manager 2.6 RKE 1.4 con Rancher Manager 2.7 RKE 2 (v1.24.x) con Rancher 2.6 RKE 2 (v1,26.x) con Rancher 2,7
Red Hat OpenShift Container Platform	da 4,11 a 4,14
VMware Tanzu Kubernetes Grid Integrated Edition	1,16.x (vedere Requisiti delle risorse del cluster host)

Requisiti delle risorse del cluster host

Astra Control Center richiede le seguenti risorse oltre ai requisiti delle risorse dell'ambiente:

> Questi requisiti presuppongono che Astra Control Center sia l'unica applicazione in esecuzione nell'ambiente operativo. Se nell'ambiente sono in esecuzione applicazioni aggiuntive, modificare di conseguenza questi requisiti minimi.

- **CPU Extensions**: Le CPU di tutti i nodi dell'ambiente di hosting devono avere le estensioni AVX abilitate.
- **Nodi di lavoro**: Almeno 3 nodi di lavoro in totale, con 4 core CPU e 12 GB di RAM ciascuno
- **Requisiti del cluster VMware Tanzu Kubernetes Grid**: Quando si ospita Astra Control Center su un cluster VMware Tanzu Kubernetes Grid (TKG) o Tanzu Kubernetes Grid Integrated Edition (TKGi), tenere presente le seguenti considerazioni.
  - Il token del file di configurazione predefinito di VMware TKG e TKGi scade dieci ore dopo l'implementazione. Se si utilizzano prodotti del portfolio Tanzu, è necessario generare un file di configurazione del cluster Tanzu Kubernetes con un token non in scadenza per evitare problemi di connessione tra Astra Control Center e cluster di applicazioni gestiti. Per istruzioni, visitare il sito "Documentazione del prodotto VMware NSX-T Data Center."
  - Utilizzare `kubectl get nsxlbmonitors -A` per verificare se è già stato configurato un monitor dei servizi per accettare il traffico in entrata. Se ne esiste uno, non installare MetalLB, perché il monitor di servizio esistente sovrascriverà qualsiasi nuova configurazione del bilanciamento del carico.
  - Disattivare l'applicazione della classe di storage predefinita TKG o TKGi su qualsiasi cluster di applicazioni che deve essere gestito da Astra Control. Per eseguire questa operazione, modificare il `TanzuKubernetesCluster` risorsa sul cluster dello spazio dei nomi.
  - Quando si implementa Astra Control Center in un ambiente TKG o TKGi, è necessario conoscere i requisiti specifici di Astra Trident. Per ulteriori informazioni, consultare "Documentazione di Astra Trident".

Requisiti mesh di servizio

Si consiglia vivamente di installare una versione vanilla supportata della mesh di servizio Istio sul cluster host Astra Control Center. Fare riferimento a. "versioni supportate" Per le versioni supportate di Istio. Le versioni con marchio di Istio Service Mesh, come OpenShift Service Mesh, non sono validate con Astra Control Center.

Per integrare Astra Control Center con la mesh di servizio Istio installata sul cluster host, è necessario eseguire l'integrazione come parte di Astra Control Center "installazione" e non indipendente da questo processo.

L'installazione di Astra Control Service senza la configurazione di una mesh di servizio sul cluster host ha potenzialmente serie implicazioni per la sicurezza.

Requisiti di Astra Trident

Assicurati di soddisfare i seguenti requisiti di Astra Trident specifici per le esigenze del tuo ambiente:

- **Versione minima da utilizzare con Astra Control Center**: Astra Trident 23,01 o versione successiva installato e configurato
- **Configurazione ONTAP con Astra Trident**:
  - **Storage class**: Configurare almeno una classe di storage Astra Trident sul cluster. Se viene configurata una classe di storage predefinita, assicurarsi che sia l'unica classe di storage con la designazione predefinita.
  - **Driver di storage e nodi di lavoro**: Assicurarsi di configurare i nodi di lavoro nel cluster con i driver di storage appropriati in modo che i pod possano interagire con lo storage backend. Centro di controllo Astra supporta i seguenti driver ONTAP forniti da Astra Trident:
    - `ontap-nas`
    - `ontap-san`
    - `ontap-san-economy` (la replica dell'applicazione non è disponibile con questo tipo di classe di storage)
    - `ontap-nas-economy` (snapshot e policy di replica non sono disponibili con questo tipo di classe di storage)

Astra Control provisioner

Per utilizzare le funzionalità di storage avanzate di Astra Control Provivisioner, devi installare Astra Trident 23,10 o versioni successive e abilitare "Funzionalità Astra Control Provisioner".

Back-end dello storage

Assicurarsi di disporre di un backend supportato con capacità sufficiente.

- **Capacità di back-end dello storage richiesta**: Almeno 500 GB disponibili
- **Backend supportati**: Astra Control Center supporta i seguenti backend di storage:
  - NetApp ONTAP 9.9.1 o sistemi AFF, FAS e ASA più recenti
  - NetApp ONTAP Select 9.9.1 o versione successiva
  - NetApp Cloud Volumes ONTAP 9.9.1 o versione successiva
  - Longhorn 1.5.0 o versione successiva
    - Richiede la creazione manuale di un oggetto VolumeSnapshotClass. Fare riferimento a. "Documentazione di Longhorn" per istruzioni.
  - NetApp MetroCluster
    - I cluster Kubernetes gestiti devono essere in una configurazione stretch.
  - Backend di storage disponibili con cloud provider supportati

Licenze ONTAP

Per utilizzare il centro di controllo Astra, verificare di disporre delle seguenti licenze ONTAP, a seconda delle operazioni da eseguire:

- FlexClone
- SnapMirror: Opzionale. Necessario solo per la replica su sistemi remoti utilizzando la tecnologia SnapMirror. Fare riferimento a. "Informazioni sulla licenza SnapMirror".
- Licenza S3: Opzionale. Necessario solo per i bucket ONTAP S3

Per verificare se il sistema ONTAP dispone delle licenze richieste, fare riferimento a. "Gestire le licenze ONTAP".

NetApp MetroCluster

Quando utilizzi NetApp MetroCluster come back-end dello storage, devi quanto segue:

- Specifica una LIF di gestione SVM come opzione di backend nel driver Astra Trident che utilizzi
- Assicurarsi di disporre della licenza ONTAP appropriata

Per configurare il file LIF di MetroCluster, consultare la documentazione di Astra Trident per ulteriori informazioni su ciascun driver:

- "SAN"
- "NAS"

Registro delle immagini

È necessario disporre di un registro di immagini Docker privato in cui è possibile trasferire le immagini di build di Astra Control Center. È necessario fornire l'URL del registro delle immagini in cui verranno caricate le immagini.

Licenza Astra Control Center

Astra Control Center richiede una licenza Astra Control Center. Quando si installa Astra Control Center, viene già attivata una licenza di valutazione integrata di 90 giorni per 4,800 unità CPU. Se hai bisogno di una maggiore capacità o di termini di valutazione diversi, o se desideri passare a una licenza completa, puoi ottenere una licenza di valutazione o una licenza completa diversa da NetApp. Hai bisogno di una licenza per proteggere le tue applicazioni e i tuoi dati.

Puoi provare Astra Control Center registrandoti per una prova gratuita. Puoi iscriverti registrandoti "qui".

Per impostare la licenza, fare riferimento a. "utilizzare una licenza di valutazione di 90 giorni".

Per ulteriori informazioni sul funzionamento delle licenze, fare riferimento a. "Licensing".

Requisiti di rete

Configura il tuo ambiente operativo per garantire che Astra Control Center possa comunicare correttamente. Sono necessarie le seguenti configurazioni di rete:

- **Indirizzo FQDN**: È necessario disporre di un indirizzo FQDN per Astra Control Center.

- **Accesso a Internet**: È necessario determinare se si dispone di accesso esterno a Internet. In caso contrario, alcune funzionalità potrebbero essere limitate, ad esempio la ricezione di dati di monitoraggio e metriche da NetApp Cloud Insights o l'invio di pacchetti di supporto a "Sito di supporto NetApp".
- **Port Access**: L'ambiente operativo che ospita Astra Control Center comunica utilizzando le seguenti porte TCP. Assicurarsi che queste porte siano consentite attraverso qualsiasi firewall e configurare i firewall in modo da consentire qualsiasi traffico HTTPS in uscita dalla rete Astra. Alcune porte richiedono la connettività tra l'ambiente che ospita Astra Control Center e ciascun cluster gestito (annotato dove applicabile).

Puoi implementare Astra Control Center in un cluster Kubernetes dual-stack, mentre Astra Control Center può gestire le applicazioni e i back-end di storage configurati per il funzionamento dual-stack. Per ulteriori informazioni sui requisiti del cluster dual-stack, vedere "Documentazione Kubernetes".

Origine	Destinazione	Porta	Protocollo	Scopo
PC client	Centro di controllo Astra	443	HTTPS	Accesso UI/API - assicurarsi che questa porta sia aperta in entrambe le direzioni tra Astra Control Center e il sistema utilizzato per accedere ad Astra Control Center
Metriche consumer	Nodo di lavoro Astra Control Center	9090	HTTPS	Comunicazione dei dati delle metriche - garantire che ciascun cluster gestito possa accedere a questa porta sul cluster che ospita Astra Control Center (è richiesta una comunicazione bidirezionale)
Centro di controllo Astra	Servizio Hosted Cloud Insights (https://www.netapp.com/cloud-services/cloud-insights/)	443	HTTPS	Comunicazione Cloud Insights
Centro di controllo Astra	Provider di bucket di storage Amazon S3	443	HTTPS	Comunicazione con lo storage Amazon S3
Centro di controllo Astra	NetApp AutoSupport (https://support.netapp.com)	443	HTTPS	Comunicazioni NetApp AutoSupport

Origine	Destinazione	Porta	Protocollo	Scopo
Centro di controllo Astra	Cluster Kubernetes gestito	443/6443 **NOTA**: La porta utilizzata dal cluster gestito può variare a seconda del cluster. Fare riferimento alla documentazione fornita dal fornitore del software per cluster.	HTTPS	Comunicazione con il cluster gestito - assicurarsi che questa porta sia aperta in entrambi i modi tra il cluster che ospita Astra Control Center e ciascun cluster gestito

Ingresso per cluster Kubernetes on-premise

È possibile scegliere il tipo di ingresso di rete utilizzato da Astra Control Center. Per impostazione predefinita, Astra Control Center implementa il gateway Astra Control Center (servizio/traefik) come risorsa a livello di cluster. Astra Control Center supporta anche l'utilizzo di un servizio di bilanciamento del carico, se consentito nel tuo ambiente. Se si preferisce utilizzare un servizio di bilanciamento del carico e non ne si dispone già di uno configurato, è possibile utilizzare il bilanciamento del carico MetalLB per assegnare automaticamente un indirizzo IP esterno al servizio. Nella configurazione del server DNS interno, puntare il nome DNS scelto per Astra Control Center sull'indirizzo IP con bilanciamento del carico.

> Il bilanciamento del carico deve utilizzare un indirizzo IP situato nella stessa subnet degli indirizzi IP del nodo di lavoro di Astra Control Center.

Per ulteriori informazioni, fare riferimento a. "Impostare l'ingresso per il bilanciamento del carico".

Requisiti di ingresso di Google anthos

Quando si ospita Astra Control Center su un cluster Google anthos, Google anthos include il bilanciamento del carico MetalLB e il servizio di ingresso Istio per impostazione predefinita, consentendo di utilizzare semplicemente le funzionalità di ingresso generiche di Astra Control Center durante l'installazione. Fare riferimento a. "Configurare Astra Control Center" per ulteriori informazioni.

Browser Web supportati

Astra Control Center supporta versioni recenti di Firefox, Safari e Chrome con una risoluzione minima di 1280 x 720.

Requisiti aggiuntivi per i cluster di applicazioni

Se si prevede di utilizzare queste funzionalità di Astra Control Center, tenere presenti questi requisiti:

- **Requisiti del cluster applicativo**: "Requisiti di gestione del cluster"
  - **Requisiti delle applicazioni gestite**: "Requisiti di gestione delle applicazioni"
  - **Requisiti aggiuntivi per la replica delle applicazioni**: "Prerequisiti per la replica"

Cosa succederà

Visualizzare il "avvio rapido" panoramica.

Avvio rapido per Astra Control Center

Ecco una panoramica dei passaggi necessari per iniziare a utilizzare Astra Control Center. I collegamenti all'interno di ogni passaggio consentono di accedere a una pagina che fornisce ulteriori dettagli.

Esaminare i requisiti del cluster Kubernetes

Assicurarsi che l'ambiente soddisfi i seguenti requisiti:

Cluster Kubernetes

- "Assicurarsi che il cluster host soddisfi i requisiti dell'ambiente operativo"
- "Configurare l'ingresso per il bilanciamento del carico dei cluster Kubernetes on-premise"

Integrazione dello storage

- "Verifica che il tuo ambiente includa una versione supportata di Astra Trident"
- "Abilita le funzionalità avanzate di gestione e provisioning dello storage di Astra Control Provisioner"
- "Preparare i nodi di lavoro"
- "Configurare il backend dello storage Astra Trident"
- "Configurare le classi di storage Astra Trident"
- "Installare il controller di snapshot del volume Astra Trident"
- "Creare una classe di snapshot di volume"

Credenziali ONTAP

- "Configurare le credenziali ONTAP"

Scaricare e installare Astra Control Center

Completare le seguenti attività di installazione:

- "Scarica Astra Control Center dalla pagina di download del sito di supporto NetApp"
- Ottenere il file di licenza NetApp:
  - Se si sta valutando Astra Control Center, è già inclusa una licenza di valutazione integrata
  - "Se si è già acquistato Astra Control Center, generare il file di licenza"
- "Installare Astra Control Center"
- "Eseguire ulteriori procedure di configurazione opzionali"

Completare alcune attività di configurazione iniziali

Completare alcune attività di base per iniziare:

- "Aggiungere una licenza"

- "Prepara il tuo ambiente per la gestione dei cluster"
- "Aggiungere un cluster"
- "Aggiungere un backend di storage"
- "Aggiungi un bucket"

4 **Utilizzare Astra Control Center**

Una volta completata la configurazione di Astra Control Center, utilizzare l'interfaccia utente di Astra Control o il "API di controllo Astra" per iniziare a gestire e proteggere le applicazioni:

- "Gestire le applicazioni": Definire le risorse da gestire.
- "Proteggi le app": Configurare le policy di protezione e replicare, clonare e migrare le applicazioni.
- "Gestire gli account": Utenti, ruoli, LDAP, credenziali e altro ancora.
- "In alternativa, connettersi a Cloud Insights": Consente di visualizzare le metriche sullo stato di salute del sistema.

Per ulteriori informazioni

- "Utilizzare l'API di controllo Astra"
- "Aggiornare Astra Control Center"
- "Ottieni assistenza con Astra Control"

Panoramica dell'installazione

Scegliere e completare una delle seguenti procedure di installazione di Astra Control Center:

- "Installare Astra Control Center utilizzando il processo standard"
- "(Se utilizzi Red Hat OpenShift) Installa Astra Control Center usando OpenShift OperatorHub"
- "Installare il centro di controllo Astra con un backend di storage Cloud Volumes ONTAP"

A seconda dell'ambiente in uso, potrebbe essere necessaria una configurazione aggiuntiva dopo l'installazione di Astra Control Center:

- "Configurare Astra Control Center dopo l'installazione"

Installare Astra Control Center utilizzando il processo standard

Per installare Astra Control Center, scaricare il pacchetto di installazione dal NetApp Support Site ed eseguire la seguente procedura. È possibile utilizzare questa procedura per installare Astra Control Center in ambienti connessi a Internet o con connessione ad aria.

Espandere per altre procedure di installazione

- **Installa con Red Hat OpenShift OperatorHub**: USA questo "procedura alternativa" Per installare Astra Control Center su OpenShift utilizzando OperatorHub.
- **Installare nel cloud pubblico con backend Cloud Volumes ONTAP**: Utilizzare "queste procedure" Per installare Astra Control Center in Amazon Web Services (AWS), Google Cloud Platform (GCP) o Microsoft Azure con un backend di storage Cloud Volumes ONTAP.

Per una dimostrazione del processo di installazione di Astra Control Center, vedere "questo video".

Prima di iniziare

- **Soddisfare i requisiti ambientali**: "Prima di iniziare l'installazione, preparare l'ambiente per l'implementazione di Astra Control Center".

  Implementare Astra Control Center in un terzo dominio di errore o in un sito secondario. Questa opzione è consigliata per la replica delle applicazioni e il disaster recovery perfetto.

- **Garantire servizi integri**: Controllare che tutti i servizi API siano in buono stato e disponibili:

```
kubectl get apiservices
```

- **Assicurarsi che un FQDN instradabile**: Il FQDN Astra che si intende utilizzare può essere instradato al cluster. Ciò significa che si dispone di una voce DNS nel server DNS interno o si sta utilizzando un percorso URL principale già registrato.
- **Configure cert manager**: Se nel cluster esiste già un cert manager, è necessario eseguirne alcuni "fasi preliminari" In modo che Astra Control Center non tenti di installare il proprio cert manager. Per impostazione predefinita, Astra Control Center installa il proprio cert manager durante l'installazione.
- **Accedere al Registro di sistema dell'immagine di controllo Astra di NetApp**:
  È possibile ottenere le immagini di installazione e i miglioramenti delle funzionalità per Astra Control, come Astra Control provisioner, dal registro delle immagini di NetApp.

  Espandere per i passaggi

  a. Registrare l'ID dell'account Astra Control necessario per accedere al Registro di sistema.

     Puoi visualizzare l'ID dell'account nell'interfaccia utente Web di Astra Control Service. Selezionare l'icona a forma di figura in alto a destra nella pagina, selezionare **accesso API** e annotare l'ID account.

  b. Nella stessa pagina, selezionare **generate API token**, copiare la stringa del token API negli Appunti e salvarla nell'editor.

  c. Accedere al registro Astra Control:

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

- **Considerare una mesh di servizio**: Si consiglia vivamente di proteggere i canali di comunicazione del

cluster host Astra Control utilizzando un "mesh di servizio supportata".

Dettagli mesh di servizio Istio

Per l'uso della mesh del servizio Istio, è necessario effettuare le seguenti operazioni:

- Aggiungere un `istio-injection:enabled` etichetta Al namespace Astra prima di implementare Astra Control Center.
- Utilizzare `Generic` impostazione ingresso e fornire un ingresso alternativo per bilanciamento del carico esterno.
- Per i cluster Red Hat OpenShift, è necessario definire `NetworkAttachmentDefinition` Su tutti i namespace Astra Control Center associati (`netapp-acc-operator`, `netapp-acc`, `netapp-monitoring` per i cluster di applicazioni o qualsiasi namespace personalizzato che sia stato sostituito).

```
cat <<EOF | oc -n netapp-acc-operator create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF

cat <<EOF | oc -n netapp-acc create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF

cat <<EOF | oc -n netapp-monitoring create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF
```

- **Solo driver SAN ONTAP**: Se stai utilizzando un driver SAN ONTAP, assicurati che multipath sia abilitato su tutti i tuoi cluster Kubernetes.

Fasi

Per installare Astra Control Center, procedere come segue:

- Scarica ed estrai Astra Control Center
- Installare il plug-in NetApp Astra kubectl
- Aggiungere le immagini al registro locale

- Impostare namespace e secret per i registri con requisiti di autenticazione
- Installare l'operatore del centro di controllo Astra
- Configurare Astra Control Center
- Completare l'installazione dell'Astra Control Center e dell'operatore
- Verificare lo stato del sistema
- Impostare l'ingresso per il bilanciamento del carico
- Accedere all'interfaccia utente di Astra Control Center

> Non eliminare l'operatore di Astra Control Center (ad esempio, `kubectl delete -f astra_control_center_operator_deploy.yaml`) In qualsiasi momento durante l'installazione o il funzionamento di Astra Control Center per evitare di eliminare i pod.

Scarica ed estrai Astra Control Center

Puoi scegliere di scaricare il bundle Astra Control Center dal sito di supporto di NetApp o utilizzare Docker per estrarre il bundle dal registro delle immagini di Astra Control Service.

Sito di supporto NetApp

1. Scarica il bundle contenente Astra Control Center (`astra-control-center-[version].tar.gz`) da "Pagina di download di Astra Control Center".
2. (Consigliato ma opzionale) Scarica il bundle di certificati e firme per Astra Control Center (`astra-control-center-certs-[version].tar.gz`) per verificare la firma del bundle.

   Espandere per i dettagli

   ```
   tar -vxzf astra-control-center-certs-[version].tar.gz
   ```

   ```
   openssl dgst -sha256 -verify certs/AstraControlCenter-public.pub
   -signature certs/astra-control-center-[version].tar.gz.sig
   astra-control-center-[version].tar.gz
   ```

   Viene visualizzato l'output `Verified OK` una volta completata la verifica.

3. Estrarre le immagini dal bundle Astra Control Center:

   ```
   tar -vxzf astra-control-center-[version].tar.gz
   ```

Registro delle immagini di Astra Control

1. Effettua l'accesso ad Astra Control Service.
2. Nella Dashboard, selezionare **distribuire un'istanza autogestita di Astra Control**.
3. Seguire le istruzioni per accedere al registro delle immagini di Astra Control, estrarre l'immagine di installazione di Astra Control Center ed estrarre l'immagine.

Installare il plug-in NetApp Astra kubectl

È possibile utilizzare il plug-in della riga di comando di NetApp Astra kubectl per inviare immagini a un repository Docker locale.

Prima di iniziare

NetApp fornisce binari per plug-in per diverse architetture CPU e sistemi operativi. Prima di eseguire questa attività, è necessario conoscere la CPU e il sistema operativo in uso.

Se il plug-in è già stato installato da un'installazione precedente, "assicurarsi di disporre della versione più recente" prima di completare questa procedura.

Fasi

1. Elencare i binari disponibili per il plugin NetApp Astra kubectl:

La libreria di plugin kubectl fa parte del bundle tar e viene estratta nella cartella `kubectl-astra`.

```
ls kubectl-astra/
```

2. Spostare il file necessario per il sistema operativo e l'architettura della CPU nel percorso corrente e rinominarlo `kubectl-astra`:

```
cp kubectl-astra/<binary-name> /usr/local/bin/kubectl-astra
```

Aggiungere le immagini al registro locale

1. Completare la sequenza di passaggi appropriata per il motore dei container:

Docker

1. Passare alla directory root del tarball. Viene visualizzata la `acc.manifest.bundle.yaml` file e queste directory:

   ```
   acc/
   kubectl-astra/
   acc.manifest.bundle.yaml
   ```

2. Trasferire le immagini del pacchetto nella directory delle immagini di Astra Control Center nel registro locale. Eseguire le seguenti sostituzioni prima di eseguire `push-images` comando:

   - Sostituire <BUNDLE_FILE> con il nome del file bundle di controllo Astra (`acc.manifest.bundle.yaml`).
   - Sostituire <MY_FULL_REGISTRY_PATH> con l’URL del repository Docker; ad esempio, "<a href="https://<docker-registry>"" class="bare">https://<docker-registry>".
   - Sostituire <MY_REGISTRY_USER> con il nome utente.
   - Sostituire <MY_REGISTRY_TOKEN> con un token autorizzato per il registro.

   ```
   kubectl astra packages push-images -m <BUNDLE_FILE> -r
   <MY_FULL_REGISTRY_PATH> -u <MY_REGISTRY_USER> -p
   <MY_REGISTRY_TOKEN>
   ```

Podman

1. Passare alla directory root del tarball. Vengono visualizzati il file e la directory seguenti:

   ```
   acc/
   kubectl-astra/
   acc.manifest.bundle.yaml
   ```

2. Accedere al Registro di sistema:

   ```
   podman login <YOUR_REGISTRY>
   ```

3. Preparare ed eseguire uno dei seguenti script personalizzato per la versione di Podman utilizzata. Sostituire <MY_FULL_REGISTRY_PATH> con l'URL del repository che include le sottodirectory.

   ```
   <strong>Podman 4</strong>
   ```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.10.0-68
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done
```

```
<strong>Podman 3</strong>
```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.10.0-68
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done
```

Il percorso dell'immagine creato dallo script deve essere simile al seguente, a seconda della configurazione del Registro di sistema:

```
https://downloads.example.io/docker-astra-control-
prod/netapp/astra/acc/23.10.0-68/image:version
```

Impostare namespace e secret per i registri con requisiti di autenticazione

1. Esportare il file kubeconfig per il cluster host Astra Control Center:

```
export KUBECONFIG=[file path]
```

Prima di completare l'installazione, assicurarsi che kubeconfig punti al cluster in cui si desidera installare Astra Control Center.

2. Se si utilizza un registro che richiede l'autenticazione, è necessario effettuare le seguenti operazioni:

Espandere per i passaggi

a. Creare il `netapp-acc-operator` spazio dei nomi:

```
kubectl create ns netapp-acc-operator
```

b. Creare un segreto per `netapp-acc-operator` namespace. Aggiungere informazioni su Docker ed eseguire il seguente comando:

Il segnaposto `your_registry_path` deve corrispondere alla posizione delle immagini caricate in precedenza (ad esempio, `[Registry_URL]/netapp/astra/astracc/23.10.0-68`).

```
kubectl create secret docker-registry astra-registry-cred -n
netapp-acc-operator --docker-server=[your_registry_path] --docker
-username=[username] --docker-password=[token]
```

Se si elimina lo spazio dei nomi dopo la generazione del segreto, ricreare lo spazio dei nomi e rigenerare il segreto per lo spazio dei nomi.

c. Creare il `netapp-acc` namespace (o personalizzato).

```
kubectl create ns [netapp-acc or custom namespace]
```

d. Creare un segreto per `netapp-acc` namespace (o personalizzato). Aggiungere informazioni su Docker ed eseguire il seguente comando:

```
kubectl create secret docker-registry astra-registry-cred -n
[netapp-acc or custom namespace] --docker
-server=[your_registry_path] --docker-username=[username]
--docker-password=[token]
```

Installare l'operatore del centro di controllo Astra

1. Modificare la directory:

```
cd manifests
```

2. Modificare l'YAML di implementazione dell'operatore di Astra Control Center (`astra_control_center_operator_deploy.yaml`) per fare riferimento al registro locale e al segreto.

```
vim astra_control_center_operator_deploy.yaml
```

Un YAML di esempio annotato segue questi passaggi.

a. Se si utilizza un registro che richiede l'autenticazione, sostituire la riga predefinita di `imagePullSecrets: []` con i seguenti elementi:

```
imagePullSecrets: [{name: astra-registry-cred}]
```

b. Cambiare `ASTRA_IMAGE_REGISTRY` per `kube-rbac-proxy` al percorso del registro in cui sono state inviate le immagini in a. passaggio precedente.

c. Cambiare `ASTRA_IMAGE_REGISTRY` per `acc-operator-controller-manager` al percorso del registro in cui sono state inviate le immagini in a. passaggio precedente.

Espandere per l'esempio astra_control_center_operator_deploy.yaml

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
  name: acc-operator-controller-manager
  namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
  strategy:
    type: Recreate
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
      containers:
      - args:
        - --secure-listen-address=0.0.0.0:8443
        - --upstream=http://127.0.0.1:8080/
        - --logtostderr=true
        - --v=10
        image: ASTRA_IMAGE_REGISTRY/kube-rbac-proxy:v4.8.0
        name: kube-rbac-proxy
        ports:
        - containerPort: 8443
          name: https
      - args:
        - --health-probe-bind-address=:8081
        - --metrics-bind-address=127.0.0.1:8080
        - --leader-elect
        env:
        - name: ACCOP_LOG_LEVEL
          value: "2"
        - name: ACCOP_HELM_INSTALLTIMEOUT
          value: 5m
        image: ASTRA_IMAGE_REGISTRY/acc-operator:23.10.72
        imagePullPolicy: IfNotPresent
        livenessProbe:
          httpGet:
            path: /healthz
```

```
            port: 8081
          initialDelaySeconds: 15
          periodSeconds: 20
        name: manager
        readinessProbe:
          httpGet:
            path: /readyz
            port: 8081
          initialDelaySeconds: 5
          periodSeconds: 10
        resources:
          limits:
            cpu: 300m
            memory: 750Mi
          requests:
            cpu: 100m
            memory: 75Mi
        securityContext:
          allowPrivilegeEscalation: false
      imagePullSecrets: []
      securityContext:
        runAsUser: 65532
      terminationGracePeriodSeconds: 10
```

3. Installare l'operatore del centro di controllo Astra:

```
kubectl apply -f astra_control_center_operator_deploy.yaml
```

Espandi per la risposta di esempio:

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

4. Verificare che i pod siano in esecuzione:

```
kubectl get pods -n netapp-acc-operator
```

Configurare Astra Control Center

1. Modificare il file delle risorse personalizzate (CR) di Astra Control Center (`astra_control_center.yaml`) per creare account, supporto, registro e altre configurazioni necessarie:

```
vim astra_control_center.yaml
```

> Un YAML di esempio annotato segue questi passaggi.

2. Modificare o confermare le seguenti impostazioni:

<code>accountName</code>

Impostazione	Guida	Tipo	Esempio
`accountName`	Modificare il `accountName` Stringa al nome che si desidera associare all'account Astra Control Center. Può essere presente un solo nome account.	stringa	`Example`

<code>astraVersion</code>

Impostazione	Guida	Tipo	Esempio
`astraVersion`	La versione di Astra Control Center da implementare. Non è necessaria alcuna azione per questa impostazione, in quanto il valore verrà pre-compilato.	stringa	`23.10.0-68`

<code>astraAddress</code>

Impostazione	Guida	Tipo	Esempio
`astraAddress`	Modificare il `astraAddress` Inserire l'FQDN (consigliato) o l'indirizzo IP che si desidera utilizzare nel browser per accedere ad Astra Control Center. Questo indirizzo definisce il modo in cui Astra Control Center verrà trovato nel data center e corrisponde allo stesso FQDN o indirizzo IP fornito dal bilanciamento del carico al termine dell'operazione "Requisiti di Astra Control Center". NOTA: Non utilizzare `http://` oppure `https://` nell'indirizzo. Copiare questo FQDN per utilizzarlo in un passo successivo.	stringa	`astra.example.com`

<code>autoSupport</code>

Le selezioni effettuate in questa sezione determinano se parteciperete all'applicazione di supporto proattiva di NetApp, il consulente digitale e la posizione in cui vengono inviati i dati. È necessaria una connessione a Internet (porta 442) e tutti i dati di supporto sono resi anonimi.

Impostazione	Utilizzare	Guida	Tipo	Esempio
`autoSupport.enrolled`	Entrambi `enrolled` oppure `url` i campi devono essere selezionati	Cambiare `enrolled` Per AutoSupport a. `false` per i siti senza connettività internet o senza retain `true` per i siti connessi. Un'impostazione di `true` Consente l'invio di dati anonimi a NetApp a scopo di supporto. L'elezione predefinita è `false` E indica che non verranno inviati dati di supporto a NetApp.	Booleano	`false` (valore predefinito)
`autoSupport.url`	Entrambi `enrolled` oppure `url` i campi devono essere selezionati	Questo URL determina dove verranno inviati i dati anonimi.	stringa	`https://support.netapp.com/asupprod/post/1.0/postAsup`

<code>email</code>

Impostazione	Guida	Tipo	Esempio
`email`	Modificare il `email` stringa all'indirizzo iniziale predefinito dell'amministratore. Copiare questo indirizzo e-mail per utilizzarlo in passo successivo. Questo indirizzo e-mail verrà utilizzato come nome utente per l'account iniziale per accedere all'interfaccia utente e verrà notificato degli eventi in Astra Control.	stringa	`admin@example.com`

<code>firstName</code>

Impostazione	Guida	Tipo	Esempio
`firstName`	Il nome dell'amministratore iniziale predefinito associato all'account Astra. Il nome utilizzato qui sarà visibile in un'intestazione dell'interfaccia utente dopo il primo accesso.	stringa	`SRE`

<code>LastName</code>

Impostazione	Guida	Tipo	Esempio
`lastName`	Il cognome dell'amministratore iniziale predefinito associato all'account Astra. Il nome utilizzato qui sarà visibile in un'intestazione dell'interfaccia utente dopo il primo accesso.	stringa	`Admin`

<code>imageRegistry</code>

Le selezioni effettuate in questa sezione definiscono il registro delle immagini container che ospita le immagini dell'applicazione Astra, Astra Control Center Operator e il repository Astra Control Center Helm.

Impostazione	Utilizzare	Guida	Tipo	Esempio
`imageRegistry.name`	Obbligatorio	Il nome del registro delle immagini in cui sono state inviate le immagini in passaggio precedente. Non utilizzare `http://` oppure `https://` nel nome del registro di sistema.	stringa	`example.registry.com/astra`
`imageRegistry.secret`	Obbligatorio se la stringa immessa per `imageRegistry.name' requires a secret.` `IMPORTANT: If you are using a registry that does not require authorization, you must delete this` `secret` linea entro `imageRegistry` in caso negativo, l'installazione non riesce.	Il nome del segreto Kubernetes utilizzato per l'autenticazione con il registro delle immagini.	stringa	`astra-registry-cred`

<code>storageClass</code>

Impostazione	Guida	Tipo	Esempio
`storageClass`	Modificare il `storageClass` valore da `ontap-gold` A un'altra risorsa Astra Trident storageClass come richiesto dall'installazione. Eseguire il comando `kubectl get sc` per determinare le classi di storage configurate esistenti. Una delle classi di storage basate su Astra Trident deve essere inserita nel file manifest (`astra-control-center-<version>.manifest`) E verranno utilizzati per Astra PVS. Se non è impostata, viene utilizzata la classe di storage predefinita. NOTA: Se è configurata una classe di storage predefinita, assicurarsi che sia l'unica classe di storage con l'annotazione predefinita.	stringa	`ontap-gold`

<code>volumeReclaimPolicy</code>

Impostazione	Guida	Tipo	Opzioni
`volumeReclaimPolicy`	In questo modo viene impostata la policy di recupero per il PVS di Astra. Impostare questo criterio su `Retain` Conserva i volumi persistenti dopo l'eliminazione di Astra. Impostare questo criterio su `Delete` elimina i volumi persistenti dopo l'eliminazione di astra. Se questo valore non viene impostato, il PVS viene mantenuto.	stringa	• `Retain` (Valore predefinito) • `Delete`

<code>ingressType</code>

Impostazione	Guida	Tipo	Opzioni
`ingressType`	Utilizzare uno dei seguenti tipi di ingresso: `Generic`* (`ingressType: "Generic"`) (Impostazione predefinita) Utilizzare questa opzione quando si utilizza un altro controller di ingresso o si preferisce utilizzare un controller di ingresso personalizzato. Una volta implementato Astra Control Center, è necessario configurare "controller di ingresso" Per esporre Astra Control Center con un URL. IMPORTANTE: Se si intende utilizzare una mesh di servizio con Astra Control Center, è necessario selezionare `Generic` come tipo di ingresso e configurare il proprio "controller di ingresso". **`AccTraefik`** (`ingressType: "AccTraefik"`) Utilizzare questa opzione quando si preferisce non configurare un controller di ingresso. In questo modo viene implementato l'Astra Control Center `traefik` Gateway come servizio di tipo Kubernetes LoadBalancer. Astra Control Center utilizza un servizio del tipo "LoadBalancer" (`svc/traefik` Nello	stringa	• `Generic` (valore predefinito) • `AccTraefik`

<code>scaleSize</code>

Impostazione	Guida	Tipo	Opzioni
`scaleSize`	Per impostazione predefinita, Astra utilizza High Availability (ha) `scaleSize` di `Medium`, Che implementa la maggior parte dei servizi in ha e implementa più repliche per la ridondanza. Con `scaleSize` come `Small`, Astra ridurrà il numero di repliche per tutti i servizi ad eccezione dei servizi essenziali per ridurre il consumo. SUGGERIMENTO: `Medium` le implementazioni sono costituite da circa 100 pod (non inclusi i carichi di lavoro transitori. 100 pod si basa su una configurazione a tre nodi master e tre nodi worker). Tenere a conoscenza dei limiti di rete per pod che potrebbero rappresentare un problema nell'ambiente, in particolare quando si prendono in considerazione scenari di disaster recovery.	stringa	• `Small` • `Medium` (Valore predefinito)

<code>astraResourcesScaler</code>

Impostazione	Guida	Tipo	Opzioni
`astraResourcesScaler`	Opzioni di scalabilità per i limiti delle risorse di AstraControlCenter. Per impostazione predefinita, Astra Control Center implementa le richieste di risorse impostate per la maggior parte dei componenti all'interno di Astra. Questa configurazione consente allo stack software Astra Control Center di migliorare le prestazioni in ambienti con maggiore carico e scalabilità delle applicazioni. Tuttavia, negli scenari che utilizzano cluster di sviluppo o test più piccoli, il campo CR `astraResourcesScalar` può essere impostato su `Off`. In questo modo vengono disattivate le richieste di risorse e viene eseguita l'implementazione su cluster più piccoli.	stringa	• `Default` (Valore predefinito) • `Off`

<code>additionalValues</code>

Aggiungere i seguenti valori aggiuntivi ad Astra Control Center CR per evitare un problema noto durante l'installazione:

```
additionalValues:
    keycloak-operator:
      livenessProbe:
        initialDelaySeconds: 180
      readinessProbe:
        initialDelaySeconds: 180
```

- Per le comunicazioni Cloud Insights e Centro di controllo Astral, la verifica del certificato TLS è disattivata per impostazione predefinita. È possibile attivare la verifica della certificazione TLS per la comunicazione tra Cloud Insights e il cluster host e il cluster gestito di Astra Control Center aggiungendo la seguente sezione in `additionalValues`.

```
  additionalValues:
    netapp-monitoring-operator:
      config:
        ciSkipTlsVerify: false
    cloud-insights-service:
      config:
        ciSkipTlsVerify: false
    telemetry-service:
      config:
        ciSkipTlsVerify: false
```

<code>crds</code>

Le selezioni effettuate in questa sezione determinano il modo in cui Astra Control Center deve gestire i CRD.

Impostazione	Guida	Tipo	Esempio
`crds.externalCertManager`	Se si utilizza un gestore esterno dei certificati, cambiare `externalCertManager` a. `true`. L'impostazione predefinita `false` Fa in modo che Astra Control Center installi i propri CRD di gestione dei certificati durante l'installazione. I CRDS sono oggetti a livello di cluster e l'installazione potrebbe avere un impatto su altre parti del cluster. È possibile utilizzare questo indicatore per segnalare ad Astra Control Center che questi CRD verranno installati e gestiti dall'amministratore del cluster al di fuori di Astra Control Center.	Booleano	`False` (valore predefinito)
`crds.externalTraefik`	Per impostazione predefinita, Astra Control Center installerà i CRD Traefik richiesti. I CRDS sono oggetti a livello di cluster e l'installazione potrebbe avere un impatto su altre parti del cluster. È possibile utilizzare questo indicatore per segnalare ad Astra Control Center che questi CRD verranno installati e gestiti dall'amministratore del cluster al di fuori di Astra Control Center.	Booleano	`False` (valore predefinito)

Assicurarsi di aver selezionato la classe di storage e il tipo di ingresso corretti per la configurazione prima di completare l'installazione.

Espandere per l'esempio astra_control_center.yaml

```
apiVersion: astra.netapp.io/v1
kind: AstraControlCenter
metadata:
  name: astra
spec:
  accountName: "Example"
  astraVersion: "ASTRA_VERSION"
  astraAddress: "astra.example.com"
  autoSupport:
    enrolled: true
  email: "[admin@example.com]"
  firstName: "SRE"
  lastName: "Admin"
  imageRegistry:
    name: "[your_registry_path]"
    secret: "astra-registry-cred"
  storageClass: "ontap-gold"
  volumeReclaimPolicy: "Retain"
  ingressType: "Generic"
  scaleSize: "Medium"
  astraResourcesScaler: "Default"
  additionalValues:
    keycloak-operator:
      livenessProbe:
        initialDelaySeconds: 180
      readinessProbe:
        initialDelaySeconds: 180
  crds:
    externalTraefik: false
    externalCertManager: false
```

Completare l'installazione dell'Astra Control Center e dell'operatore

1. Se non lo si è già fatto in un passaggio precedente, creare il `netapp-acc` namespace (o personalizzato):

```
kubectl create ns [netapp-acc or custom namespace]
```

2. Se si utilizza una mesh di servizio con Astra Control Center, aggiungere la seguente etichetta al `netapp-acc` o namespace personalizzato:

Il tipo di ingresso (`ingressType`) deve essere impostato su `Generic` In Astra Control Center CR prima di procedere con questo comando.

```
kubectl label ns [netapp-acc or custom namespace] istio-
injection:enabled
```

3. (Consigliato) "Attivare Strict MTLS" Per la mesh di servizio Istio:

```
kubectl apply -n istio-system -f - <<EOF
apiVersion: security.istio.io/v1beta1
kind: PeerAuthentication
metadata:
  name: default
spec:
  mtls:
    mode: STRICT
EOF
```

4. Installare Astra Control Center in `netapp-acc` spazio dei nomi (o personalizzato):

```
kubectl apply -f astra_control_center.yaml -n [netapp-acc or custom
namespace]
```

L'operatore di Astra Control Center esegue un controllo automatico dei requisiti ambientali. Mancante "requisiti" Può causare problemi di installazione o il funzionamento non corretto di Astra Control Center. Vedere sezione successiva per verificare la presenza di messaggi di avvertenza relativi al controllo automatico del sistema.

Verificare lo stato del sistema

È possibile verificare lo stato del sistema utilizzando i comandi kubectl. Se preferisci utilizzare OpenShift, puoi utilizzare comandi oc paragonabili per le fasi di verifica.

Fasi

1. Verificare che il processo di installazione non abbia prodotto messaggi di avviso relativi ai controlli di convalida:

```
kubectl get acc [astra or custom Astra Control Center CR name] -n
[netapp-acc or custom namespace] -o yaml
```

Ulteriori messaggi di avviso sono riportati anche nei registri dell'operatore di Astra Control Center.

2. Correggere eventuali problemi dell'ambiente segnalati dai controlli automatici dei requisiti.

   È possibile correggere i problemi assicurandosi che l'ambiente soddisfi i requisiti "requisiti" Per Astra Control Center.

3. Verificare che tutti i componenti del sistema siano installati correttamente.

   ```
   kubectl get pods -n [netapp-acc or custom namespace]
   ```

   Ogni pod deve avere uno stato di `Running`. L'implementazione dei pod di sistema potrebbe richiedere alcuni minuti.

Espandere per la risposta del campione

```
NAME                                          READY   STATUS
RESTARTS     AGE
acc-helm-repo-6cc7696d8f-pmhm8                1/1     Running     0
9h
activity-597fb656dc-5rd4l                     1/1     Running     0
9h
activity-597fb656dc-mqmcw                     1/1     Running     0
9h
api-token-authentication-62f84                1/1     Running     0
9h
api-token-authentication-68nlf                1/1     Running     0
9h
api-token-authentication-ztgrm                1/1     Running     0
9h
asup-669d4ddbc4-fnmwp                         1/1     Running     1
(9h ago)   9h
authentication-78789d7549-lk686               1/1     Running     0
9h
bucketservice-65c7d95496-24x7l                1/1     Running     3
(9h ago)   9h
cert-manager-c9f9fbf9f-k8zq2                  1/1     Running     0
9h
cert-manager-c9f9fbf9f-qjlzm                  1/1     Running     0
9h
cert-manager-cainjector-dbbbd8447-b5qll       1/1     Running     0
9h
cert-manager-cainjector-dbbbd8447-p5whs       1/1     Running     0
9h
cert-manager-webhook-6f97bb7d84-4722b         1/1     Running     0
9h
cert-manager-webhook-6f97bb7d84-86kv5         1/1     Running     0
9h
certificates-59d9f6f4bd-2j899                 1/1     Running     0
9h
certificates-59d9f6f4bd-9d9k6                 1/1     Running     0
9h
certificates-expiry-check-28011180--1-8lkxz   0/1     Completed   0
9h
cloud-extension-5c9c9958f8-jdhrp              1/1     Running     0
9h
cloud-insights-service-5cdd5f7f-pp8r5         1/1     Running     0
9h
composite-compute-66585789f4-hxn5w            1/1     Running     0
9h
```

```
composite-volume-68649f68fd-tb7p4             1/1     Running     0
9h
credentials-dfc844c57-jsx92                   1/1     Running     0
9h
credentials-dfc844c57-xw26s                   1/1     Running     0
9h
entitlement-7b47769b87-4jb6c                  1/1     Running     0
9h
features-854d8444cc-c24b7                     1/1     Running     0
9h
features-854d8444cc-dv6sm                     1/1     Running     0
9h
fluent-bit-ds-9tlv4                           1/1     Running     0
9h
fluent-bit-ds-bpkcb                           1/1     Running     0
9h
fluent-bit-ds-cxmwx                           1/1     Running     0
9h
fluent-bit-ds-jgnhc                           1/1     Running     0
9h
fluent-bit-ds-vtr6k                           1/1     Running     0
9h
fluent-bit-ds-vxqd5                           1/1     Running     0
9h
graphql-server-7d4b9d44d5-zdbf5               1/1     Running     0
9h
identity-6655c48769-4pwk8                     1/1     Running     0
9h
influxdb2-0                                   1/1     Running     0
9h
keycloak-operator-55479d6fc6-slvmt            1/1     Running     0
9h
krakend-f487cb465-78679                       1/1     Running     0
9h
krakend-f487cb465-rjsxx                       1/1     Running     0
9h
license-64cbc7cd9c-qxsr8                      1/1     Running     0
9h
login-ui-5db89b5589-ndb96                     1/1     Running     0
9h
loki-0                                        1/1     Running     0
9h
metrics-facade-8446f64c94-x8h7b               1/1     Running     0
9h
monitoring-operator-6b44586965-pvcl4          2/2     Running     0
9h
```

```
nats-0                                          1/1     Running     0
9h
nats-1                                          1/1     Running     0
9h
nats-2                                          1/1     Running     0
9h
nautilus-85754d87d7-756qb                       1/1     Running     0
9h
nautilus-85754d87d7-q8j7d                       1/1     Running     0
9h
openapi-5f9cc76544-7fnjm                        1/1     Running     0
9h
openapi-5f9cc76544-vzr7b                        1/1     Running     0
9h
packages-5db49f8b5-lrzhd                        1/1     Running     0
9h
polaris-consul-consul-server-0                  1/1     Running     0
9h
polaris-consul-consul-server-1                  1/1     Running     0
9h
polaris-consul-consul-server-2                  1/1     Running     0
9h
polaris-keycloak-0                              1/1     Running     2
(9h ago)   9h
polaris-keycloak-1                              1/1     Running     0
9h
polaris-keycloak-2                              1/1     Running     0
9h
polaris-keycloak-db-0                           1/1     Running     0
9h
polaris-keycloak-db-1                           1/1     Running     0
9h
polaris-keycloak-db-2                           1/1     Running     0
9h
polaris-mongodb-0                               1/1     Running     0
9h
polaris-mongodb-1                               1/1     Running     0
9h
polaris-mongodb-2                               1/1     Running     0
9h
polaris-ui-66fb99479-qp9gq                      1/1     Running     0
9h
polaris-vault-0                                 1/1     Running     0
9h
polaris-vault-1                                 1/1     Running     0
9h
```

```
polaris-vault-2                                1/1     Running     0
9h
public-metrics-76fbf9594d-zmxzw                1/1     Running     0
9h
storage-backend-metrics-7d7fbc9cb9-lmd25       1/1     Running     0
9h
storage-provider-5bdd456c4b-2fftc              1/1     Running     0
9h
task-service-87575df85-dnn2q                   1/1     Running     3
(9h ago)   9h
task-service-task-purge-28011720--1-q6w4r      0/1     Completed   0
28m
task-service-task-purge-28011735--1-vk6pd      1/1     Running     0
13m
telegraf-ds-2r2kw                              1/1     Running     0
9h
telegraf-ds-6s9d5                              1/1     Running     0
9h
telegraf-ds-96jl7                              1/1     Running     0
9h
telegraf-ds-hbp84                              1/1     Running     0
9h
telegraf-ds-plwzv                              1/1     Running     0
9h
telegraf-ds-sr22c                              1/1     Running     0
9h
telegraf-rs-4sbg8                              1/1     Running     0
9h
telemetry-service-fb9559f7b-mk9l7              1/1     Running     3
(9h ago)   9h
tenancy-559bbc6b48-5msgg                       1/1     Running     0
9h
traefik-d997b8877-7xpf4                        1/1     Running     0
9h
traefik-d997b8877-9xv96                        1/1     Running     0
9h
trident-svc-585c97548c-d25z5                   1/1     Running     0
9h
vault-controller-88484b454-2d6sr               1/1     Running     0
9h
vault-controller-88484b454-fc5cz               1/1     Running     0
9h
vault-controller-88484b454-jktld               1/1     Running     0
9h
```

4. (Facoltativo) guardare `acc-operator` registri per monitorare l'avanzamento:

```
kubectl logs deploy/acc-operator-controller-manager -n netapp-acc-
operator -c manager -f
```

> `accHost` la registrazione del cluster è una delle ultime operazioni e, in caso di errore, la distribuzione non avrà esito negativo. In caso di errore di registrazione del cluster indicato nei registri, è possibile tentare di nuovo la registrazione tramite "Aggiungere il flusso di lavoro del cluster nell'interfaccia utente" O API.

5. Una volta eseguiti tutti i pod, verificare che l'installazione sia stata eseguita correttamente (`READY` è `True`) E ottenere la password di configurazione iniziale da utilizzare quando si accede ad Astra Control Center:

```
kubectl get AstraControlCenter -n [netapp-acc or custom namespace]
```

Risposta:

```
NAME    UUID                                  VERSION     ADDRESS
READY
astra   9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f  23.10.0-68
10.111.111.111  True
```

> Copiare il valore UUID. La password è `ACC-` Seguito dal valore UUID (`ACC-[UUID]` oppure, in questo esempio, `ACC-9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f`).

Impostare l'ingresso per il bilanciamento del carico

È possibile configurare un controller di ingresso Kubernetes che gestisce l'accesso esterno ai servizi. Queste procedure forniscono esempi di configurazione per un controller di ingresso se si utilizza il valore predefinito di `ingressType: "Generic"` Nella risorsa personalizzata di Astra Control Center (`astra_control_center.yaml`). Non è necessario utilizzare questa procedura, se specificato `ingressType: "AccTraefik"` Nella risorsa personalizzata di Astra Control Center (`astra_control_center.yaml`).

Dopo l'implementazione di Astra Control Center, è necessario configurare il controller di ingresso per esporre Astra Control Center con un URL.

Le fasi di installazione variano a seconda del tipo di controller di ingresso utilizzato. Astra Control Center supporta molti tipi di controller di ingresso. Queste procedure di configurazione forniscono alcuni esempi di passaggi per alcuni tipi di controller di ingresso comuni.

Prima di iniziare

- Il necessario "controller di ingresso" dovrebbe essere già implementato.
- Il "classe di ingresso" corrispondente al controller di ingresso dovrebbe già essere creato.

Passaggi per l'ingresso di Istio

1. Configurare l'ingresso Istio.

   Questa procedura presuppone che Istio venga distribuito utilizzando il profilo di configurazione "predefinito".

2. Raccogliere o creare il certificato e il file della chiave privata desiderati per Ingress Gateway.

   È possibile utilizzare un certificato CA o autofirmato. Il nome comune deve essere l'indirizzo Astra (FQDN).

   Esempio di comando:

   ```
   openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout tls.key
   -out tls.crt
   ```

3. Crea un segreto `tls secret name` di tipo `kubernetes.io/tls` Per una chiave privata TLS e un certificato in `istio-system namespace` Come descritto in TLS secrets (segreti TLS).

   Esempio di comando:

   ```
   kubectl create secret tls [tls secret name] --key="tls.key"
   --cert="tls.crt" -n istio-system
   ```

   Il nome del segreto deve corrispondere a. `spec.tls.secretName` fornito in `istio-ingress.yaml` file.

4. Implementare una risorsa di ingresso in `netapp-acc` namespace (o personalizzato) che utilizza il tipo di risorsa v1 per uno schema (`istio-Ingress.yaml` in questo esempio):

```
apiVersion: networking.k8s.io/v1
kind: IngressClass
metadata:
  name: istio
spec:
  controller: istio.io/ingress-controller
---
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: ingress
  namespace: [netapp-acc or custom namespace]
spec:
  ingressClassName: istio
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: [ACC address]
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          service:
            name: traefik
            port:
              number: 80
```

5. Applicare le modifiche:

```
kubectl apply -f istio-Ingress.yaml
```

6. Controllare lo stato dell'ingresso:

```
kubectl get ingress -n [netapp-acc or custom namespace]
```

Risposta:

```
NAME    CLASS HOSTS             ADDRESS         PORTS   AGE
ingress istio astra.example.com 172.16.103.248  80, 443 1h
```

7. Completare l'installazione di Astra Control Center.

Procedura per il controller di ingresso Nginx

1. Creare un segreto di tipo `kubernetes.io/tls` Per una chiave privata TLS e un certificato in `netapp-acc` (o con nome personalizzato) come descritto in "Segreti TLS".
2. Implementare una risorsa income in `netapp-acc` namespace (o personalizzato) che utilizza il tipo di risorsa v1 per uno schema (`nginx-Ingress.yaml` in questo esempio):

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: netapp-acc-ingress
  namespace: [netapp-acc or custom namespace]
spec:
  ingressClassName: [class name for nginx controller]
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: <ACC address>
    http:
      paths:
        - path:
          backend:
            service:
              name: traefik
              port:
                number: 80
          pathType: ImplementationSpecific
```

3. Applicare le modifiche:

```
kubectl apply -f nginx-Ingress.yaml
```

NetApp consiglia di installare il controller nginx come implementazione piuttosto che come `daemonSet`.

Procedura per il controller di ingresso OpenShift

1. Procurarsi il certificato e ottenere la chiave, il certificato e i file CA pronti per l'uso con il percorso OpenShift.
2. Creare il percorso OpenShift:

```
oc create route edge --service=traefik --port=web -n [netapp-acc or
custom namespace] --insecure-policy=Redirect --hostname=<ACC
address> --cert=cert.pem --key=key.pem
```

Accedere all'interfaccia utente di Astra Control Center

Dopo aver installato Astra Control Center, si modifica la password dell'amministratore predefinito e si accede alla dashboard dell'interfaccia utente di Astra Control Center.

Fasi

1. In un browser, immettere l'FQDN (compreso il `https://` prefisso) utilizzato in `astraAddress` in `astra_control_center.yaml` CR quando Astra Control Center è stato installato.
2. Accettare i certificati autofirmati, se richiesto.

   È possibile creare un certificato personalizzato dopo l'accesso.

3. Nella pagina di accesso di Astra Control Center, inserire il valore utilizzato per `email` poll `astra_control_center.yaml` CR quando Astra Control Center è stato installato, seguito dalla password di configurazione iniziale (`ACC-[UUID]`).

   Se si immette una password errata per tre volte, l'account admin viene bloccato per 15 minuti.

4. Selezionare **Login**.
5. Modificare la password quando richiesto.

   Se si tratta del primo accesso e si dimentica la password e non sono stati ancora creati altri account utente amministrativi, contattare "Supporto NetApp" per assistenza per il recupero della password.

6. (Facoltativo) rimuovere il certificato TLS autofirmato esistente e sostituirlo con un "Certificato TLS personalizzato firmato da un'autorità di certificazione (CA)".

Risolvere i problemi di installazione

Se uno dei servizi è in `Error` stato, è possibile esaminare i registri. Cercare i codici di risposta API nell'intervallo da 400 a 500. Questi indicano il luogo in cui si è verificato un guasto.

Opzioni

- Per esaminare i registri dell'operatore di Astra Control Center, immettere quanto segue:

```
kubectl logs deploy/acc-operator-controller-manager -n netapp-acc-
operator -c manager -f
```

- Per controllare l'output di Astra Control Center CR:

```
kubectl get acc -n [netapp-acc or custom namespace] -o yaml
```

Cosa succederà

- (Opzionale) a seconda dell'ambiente, completare la post-installazione "fasi di configurazione".
- Completare l'implementazione eseguendo "attività di installazione".

Configurare un gestore esterno dei certificati

Se nel cluster Kubernetes esiste già un cert manager, è necessario eseguire alcuni passaggi preliminari in modo che Astra Control Center non installi il proprio cert manager.

Fasi

1. Verificare che sia installato un gestore dei certificati:

```
kubectl get pods -A | grep 'cert-manager'
```

Esempio di risposta:

```
cert-manager   essential-cert-manager-84446f49d5-sf2zd              1/1
Running    0      6d5h
cert-manager   essential-cert-manager-cainjector-66dc99cc56-9ldmt   1/1
Running    0      6d5h
cert-manager   essential-cert-manager-webhook-56b76db9cc-fjqrq      1/1
Running    0      6d5h
```

2. Creare una coppia certificato/chiave per `astraAddress` FQDN:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout tls.key -out
tls.crt
```

Esempio di risposta:

```
Generating a 2048 bit RSA private key
...................+++
.......................................+++
writing new private key to 'tls.key'
```

3. Creare un segreto con i file generati in precedenza:

```
kubectl create secret tls selfsigned-tls --key tls.key --cert tls.crt -n
<cert-manager-namespace>
```

Esempio di risposta:

```
secret/selfsigned-tls created
```

4. Creare un `ClusterIssuer` file che è **esattamente** il seguente, ma include la posizione dello spazio dei nomi in cui si trova il `cert-manager` i pod sono installati:

```
apiVersion: cert-manager.io/v1
kind: ClusterIssuer
metadata:
  name: astra-ca-clusterissuer
  namespace: <cert-manager-namespace>
spec:
  ca:
    secretName: selfsigned-tls
```

```
kubectl apply -f ClusterIssuer.yaml
```

Esempio di risposta:

```
clusterissuer.cert-manager.io/astra-ca-clusterissuer created
```

5. Verificare che il `ClusterIssuer` è venuto in su correttamente. `Ready` deve essere `True` prima di procedere:

```
kubectl get ClusterIssuer
```

Esempio di risposta:

```
NAME                        READY   AGE
astra-ca-clusterissuer      True    9s
```

6. Completare il "Processo di installazione di Astra Control Center". Esiste un "Fase di configurazione richiesta per il cluster Astra Control Center YAML" In cui si modifica il valore CRD per indicare che il gestore dei certificati è installato esternamente. È necessario completare questa fase durante l'installazione in modo che Astra Control Center riconosca il cert manager esterno.

Installare Astra Control Center utilizzando OpenShift OperatorHub

Se utilizzi Red Hat OpenShift, puoi installare Astra Control Center usando l'operatore certificato Red Hat. Seguire questa procedura per installare Astra Control Center da "Catalogo Red Hat Ecosystem" Oppure utilizzando Red Hat OpenShift Container Platform.

Una volta completata questa procedura, tornare alla procedura di installazione per completare la "fasi rimanenti" per verificare che l'installazione sia riuscita e accedere.

Prima di iniziare

- **Soddisfare i requisiti ambientali**: "Prima di iniziare l'installazione, preparare l'ambiente per l'implementazione di Astra Control Center".
- **Assicurare operatori di cluster e servizi API sani**:
  - Dal cluster OpenShift, assicurati che tutti gli operatori del cluster siano in buono stato:

    ```
    oc get clusteroperators
    ```

  - Dal cluster OpenShift, assicurati che tutti i servizi API siano in buono stato:

    ```
    oc get apiservices
    ```

- **Assicurarsi che un FQDN instradabile**: Il FQDN Astra che si intende utilizzare può essere instradato al cluster. Ciò significa che si dispone di una voce DNS nel server DNS interno o si sta utilizzando un percorso URL principale già registrato.
- **Ottieni autorizzazioni OpenShift**: Avrai bisogno di tutte le autorizzazioni necessarie e dell'accesso a Red Hat OpenShift Container Platform per eseguire i passaggi di installazione descritti.
- **Configura un cert manager**: Se nel cluster esiste già un cert manager, è necessario eseguirne alcuni "fasi preliminari" In modo che Astra Control Center non installi il proprio cert manager. Per impostazione predefinita, Astra Control Center installa il proprio cert manager durante l'installazione.
- **Considerare una mesh di servizio**: Si consiglia vivamente di proteggere i canali di comunicazione del cluster host Astra Control utilizzando un "mesh di servizio supportata".

Dettagli mesh di servizio Istio

Per l'uso della mesh del servizio Istio, è necessario effettuare le seguenti operazioni:

- Aggiungere un `istio-injection:enabled` Etichetta nel namespace Astra prima di implementare Astra Control Center.
- Utilizzare `Generic` impostazione ingresso e fornire un ingresso alternativo per "bilanciamento del carico esterno".
- Per i cluster Red Hat OpenShift, è necessario definire `NetworkAttachmentDefinition` Su tutti i namespace Astra Control Center associati (`netapp-acc-operator`, `netapp-acc`, `netapp-monitoring` per i cluster di applicazioni o qualsiasi namespace personalizzato che sia stato sostituito).

```
cat <<EOF | oc -n netapp-acc-operator create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF

cat <<EOF | oc -n netapp-acc create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF

cat <<EOF | oc -n netapp-monitoring create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF
```

- **Kubernetes Ingress Controller**: Se si dispone di un controller di ingresso Kubernetes che gestisce l'accesso esterno ai servizi, come il bilanciamento del carico in un cluster, è necessario configurarlo per l'utilizzo con Astra Control Center:

a. Creare lo spazio dei nomi dell'operatore:

```
oc create namespace netapp-acc-operator
```

b. "Completare la configurazione" per il proprio tipo di controller di ingresso.

- **Solo driver SAN ONTAP**: Se stai utilizzando un driver SAN ONTAP, assicurati che multipath sia abilitato su tutti i tuoi cluster Kubernetes.

Fasi

- Scarica ed estrai Astra Control Center
- Installare il plug-in NetApp Astra kubectl
- Aggiungere le immagini al registro locale
- Individuare la pagina di installazione dell'operatore
- Installare l'operatore
- Installare Astra Control Center

Scarica ed estrai Astra Control Center

Puoi scegliere di scaricare il bundle Astra Control Center dal sito di supporto di NetApp o utilizzare Docker per estrarre il bundle dal registro delle immagini di Astra Control Service.

Sito di supporto NetApp

1. Scarica il bundle contenente Astra Control Center (`astra-control-center-[version].tar.gz`) da "Pagina di download di Astra Control Center".
2. (Consigliato ma opzionale) Scarica il bundle di certificati e firme per Astra Control Center (`astra-control-center-certs-[version].tar.gz`) per verificare la firma del bundle.

   Espandere per i dettagli

   ```
   tar -vxzf astra-control-center-certs-[version].tar.gz
   ```

   ```
   openssl dgst -sha256 -verify certs/AstraControlCenter-public.pub
   -signature certs/astra-control-center-[version].tar.gz.sig
   astra-control-center-[version].tar.gz
   ```

   Viene visualizzato l'output `Verified OK` una volta completata la verifica.

3. Estrarre le immagini dal bundle Astra Control Center:

   ```
   tar -vxzf astra-control-center-[version].tar.gz
   ```

Registro delle immagini di Astra Control

1. Effettua l'accesso ad Astra Control Service.
2. Nella Dashboard, selezionare **distribuire un'istanza autogestita di Astra Control**.
3. Seguire le istruzioni per accedere al registro delle immagini di Astra Control, estrarre l'immagine di installazione di Astra Control Center ed estrarre l'immagine.

Installare il plug-in NetApp Astra kubectl

È possibile utilizzare il plug-in della riga di comando di NetApp Astra kubectl per inviare immagini a un repository Docker locale.

Prima di iniziare

NetApp fornisce binari per plug-in per diverse architetture CPU e sistemi operativi. Prima di eseguire questa attività, è necessario conoscere la CPU e il sistema operativo in uso.

Fasi

1. Elencare i binari del plugin NetApp Astra kubectl disponibili e annotare il nome del file necessario per il sistema operativo e l'architettura della CPU:

   La libreria di plugin kubectl fa parte del bundle tar e viene estratta nella cartella `kubectl-astra`.

```
ls kubectl-astra/
```

2. Spostare il binario corretto nel percorso corrente e rinominarlo `kubectl-astra`:

```
cp kubectl-astra/<binary-name> /usr/local/bin/kubectl-astra
```

Aggiungere le immagini al registro locale

1. Completare la sequenza di passaggi appropriata per il motore dei container:

Docker

1. Passare alla directory root del tarball. Viene visualizzata la `acc.manifest.bundle.yaml` file e queste directory:

   ```
   acc/
   kubectl-astra/
   acc.manifest.bundle.yaml
   ```

2. Trasferire le immagini del pacchetto nella directory delle immagini di Astra Control Center nel registro locale. Eseguire le seguenti sostituzioni prima di eseguire `push-images` comando:

   - Sostituire <BUNDLE_FILE> con il nome del file bundle di controllo Astra (`acc.manifest.bundle.yaml`).
   - Sostituire <MY_FULL_REGISTRY_PATH> con l’URL del repository Docker; ad esempio, "<a href="https://<docker-registry>"" class="bare">https://<docker-registry>".
   - Sostituire <MY_REGISTRY_USER> con il nome utente.
   - Sostituire <MY_REGISTRY_TOKEN> con un token autorizzato per il registro.

   ```
   kubectl astra packages push-images -m <BUNDLE_FILE> -r
   <MY_FULL_REGISTRY_PATH> -u <MY_REGISTRY_USER> -p
   <MY_REGISTRY_TOKEN>
   ```

Podman

1. Passare alla directory root del tarball. Vengono visualizzati il file e la directory seguenti:

   ```
   acc/
   kubectl-astra/
   acc.manifest.bundle.yaml
   ```

2. Accedere al Registro di sistema:

   ```
   podman login <YOUR_REGISTRY>
   ```

3. Preparare ed eseguire uno dei seguenti script personalizzato per la versione di Podman utilizzata. Sostituire <MY_FULL_REGISTRY_PATH> con l'URL del repository che include le sottodirectory.

   ```
   <strong>Podman 4</strong>
   ```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.10.0-68
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done
```

```
<strong>Podman 3</strong>
```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.10.0-68
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done
```

Il percorso dell'immagine creato dallo script deve essere simile al seguente, a seconda della configurazione del Registro di sistema:

```
https://downloads.example.io/docker-astra-control-
prod/netapp/astra/acc/23.10.0-68/image:version
```

Individuare la pagina di installazione dell'operatore

1. Completare una delle seguenti procedure per accedere alla pagina di installazione dell'operatore:

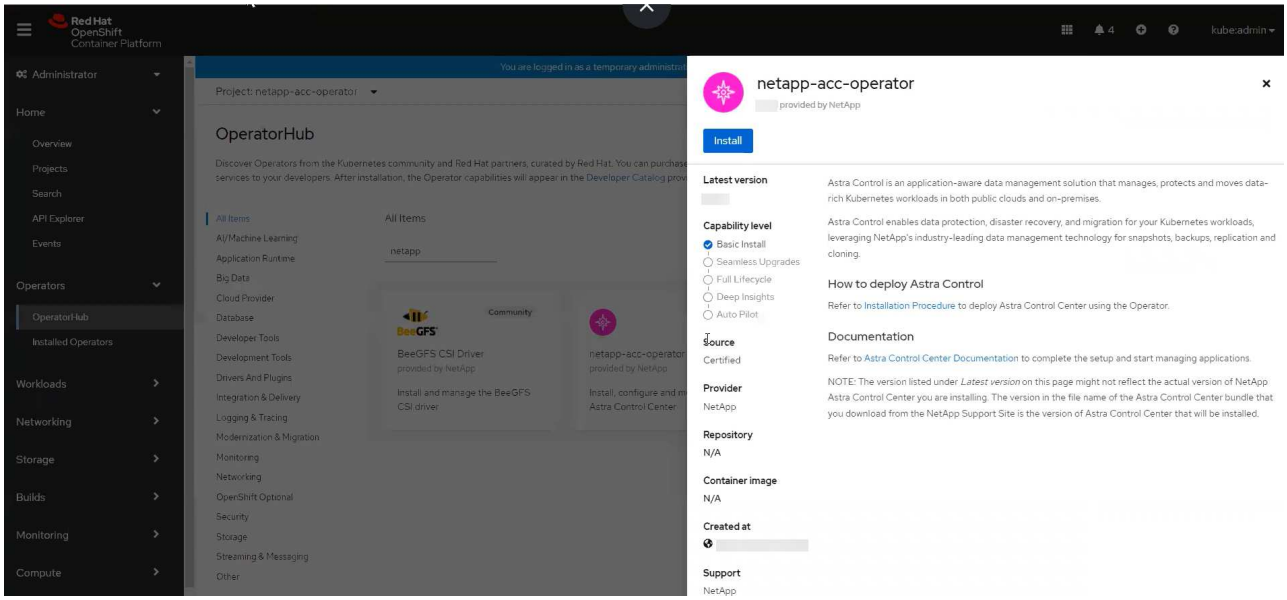
◦ Dalla console Web Red Hat OpenShift:

i. Accedere all'interfaccia utente di OpenShift Container Platform.

ii. Dal menu laterale, selezionare **Operator (operatori) > OperatorHub**.

> Con questo operatore è possibile eseguire l'aggiornamento solo alla versione corrente di Astra Control Center.

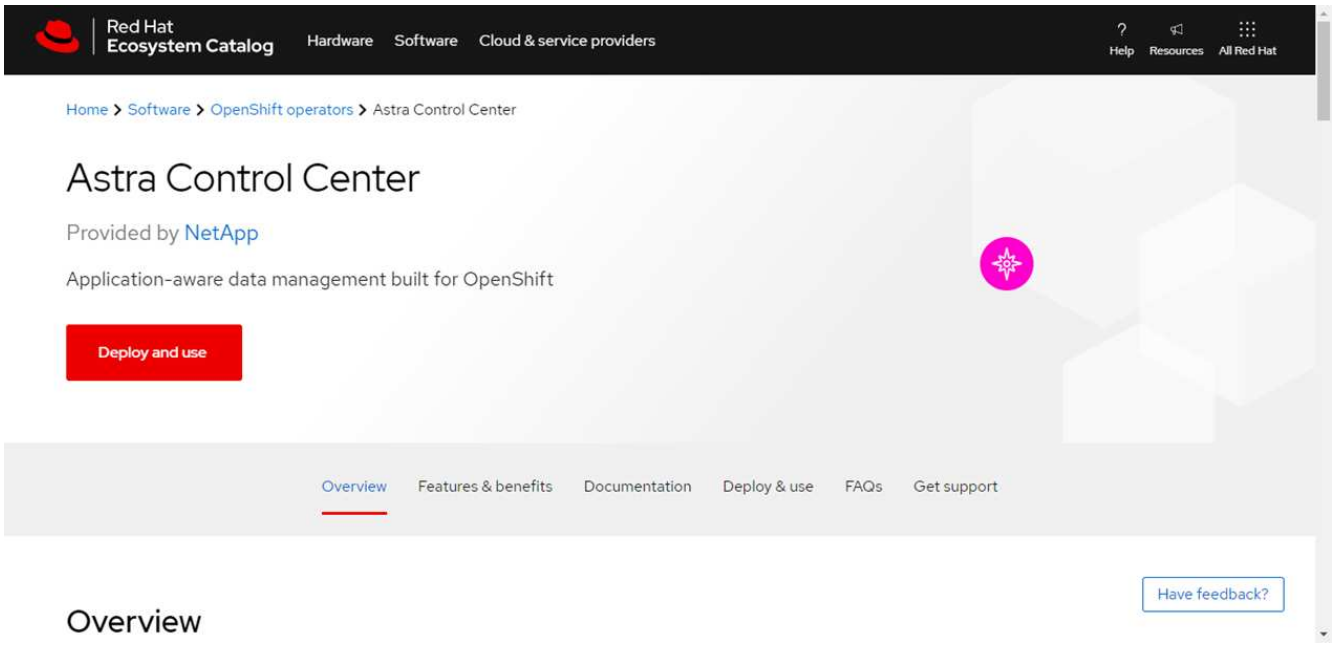
iii. Cercare e selezionare l'operatore di NetApp Astra Control Center.



◦ Dal Red Hat Ecosystem Catalog:

i. Selezionare NetApp Astra Control Center "operatore".

ii. Selezionare **Deploy and Use** (implementazione e utilizzo).



Installare l'operatore

1. Completare la pagina **Install Operator** (Installazione operatore) e installare l'operatore:

   L'operatore sarà disponibile in tutti gli spazi dei nomi dei cluster.

   a. Selezionare lo spazio dei nomi dell'operatore o. `netapp-acc-operator` lo spazio dei nomi verrà creato automaticamente come parte dell'installazione dell'operatore.

   b. Selezionare una strategia di approvazione manuale o automatica.

      Si consiglia l'approvazione manuale. Per ogni cluster dovrebbe essere in esecuzione una sola istanza dell'operatore.

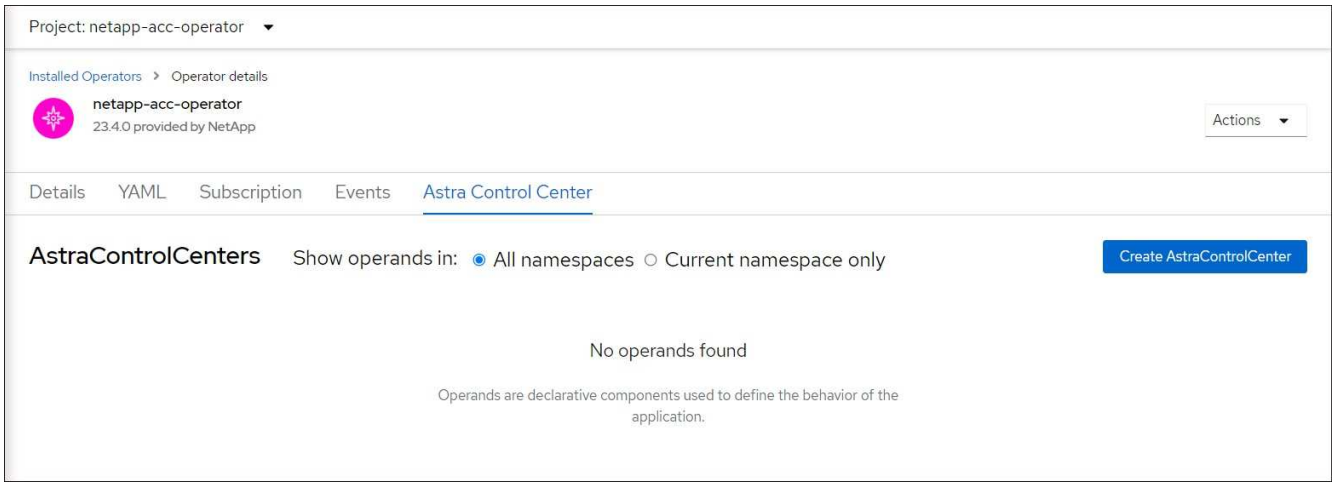
   c. Selezionare **Installa**.

      Se è stata selezionata una strategia di approvazione manuale, verrà richiesto di approvare il piano di installazione manuale per questo operatore.

2. Dalla console, accedere al menu OperatorHub e verificare che l'installazione dell'operatore sia stata eseguita correttamente.

Installare Astra Control Center

1. Dalla console all'interno della scheda **Astra Control Center** dell'operatore Astra Control Center, selezionare **Create AstraControlCenter**.



2. Completare il `Create AstraControlCenter` campo del modulo:

   a. Mantenere o regolare il nome di Astra Control Center.

   b. Aggiungere etichette per Astra Control Center.

   c. Attiva o disattiva il supporto automatico. Si consiglia di mantenere la funzionalità di supporto automatico.

   d. Inserire il nome FQDN o l'indirizzo IP di Astra Control Center. Non entrare `http://` oppure `https://` nel campo dell'indirizzo.

   e. Immettere la versione di Astra Control Center, ad esempio 23.10.0-68.

   f. Immettere un nome account, un indirizzo e-mail e un cognome amministratore.

g. Scegliere una policy di recupero dei volumi di `Retain`, `Recycle`, o. `Delete`. Il valore predefinito è `Retain`.

h. Selezionare il ScaleSize dell'installazione.

> Per impostazione predefinita, Astra utilizza High Availability (ha) `scaleSize` di `Medium`, Che implementa la maggior parte dei servizi in ha e implementa più repliche per la ridondanza. Con `scaleSize` come `Small`, Astra ridurrà il numero di repliche per tutti i servizi ad eccezione dei servizi essenziali per ridurre il consumo.

i. selezionare il tipo di ingresso:

- **`Generic`** (`ingressType: "Generic"`) (Impostazione predefinita)

  Utilizzare questa opzione quando si utilizza un altro controller di ingresso o si preferisce utilizzare un controller di ingresso personalizzato. Una volta implementato Astra Control Center, è necessario configurare "controller di ingresso" Per esporre Astra Control Center con un URL.

- **`AccTraefik`** (`ingressType: "AccTraefik"`)

  Utilizzare questa opzione quando si preferisce non configurare un controller di ingresso. In questo modo viene implementato l'Astra Control Center `traefik` Gateway come servizio di tipo Kubernetes "LoadBalancer".

Astra Control Center utilizza un servizio del tipo "LoadBalancer" (`svc/traefik` Nello spazio dei nomi di Astra Control Center) e richiede l'assegnazione di un indirizzo IP esterno accessibile. Se nel proprio ambiente sono consentiti i bilanciatori di carico e non ne è già configurato uno, è possibile utilizzare MetalLB o un altro servizio di bilanciamento del carico esterno per assegnare un indirizzo IP esterno al servizio. Nella configurazione del server DNS interno, puntare il nome DNS scelto per Astra Control Center sull'indirizzo IP con bilanciamento del carico.

> Per ulteriori informazioni sul tipo di servizio "LoadBalancer" e sull'ingresso, fare riferimento a. "Requisiti".

a. In **Image Registry**, immettere il percorso locale del Registro di sistema dell'immagine container. Non entrare `http://` oppure `https://` nel campo dell'indirizzo.

b. Se si utilizza un registro di immagini che richiede l'autenticazione, inserire il segreto dell'immagine.

> Se si utilizza un registro che richiede l'autenticazione, creare un segreto sul cluster.

c. Inserire il nome admin.

d. Configurare la scalabilità delle risorse.

e. Fornire la classe di storage predefinita.

> Se è configurata una classe di storage predefinita, assicurarsi che sia l'unica classe di storage con l'annotazione predefinita.

f. Definire le preferenze di gestione CRD.

3. Selezionare la vista YAML per rivedere le impostazioni selezionate.
4. Selezionare `Create`.

Creare un segreto di registro

Se si utilizza un registro che richiede l'autenticazione, creare un segreto nel cluster OpenShift e immettere il nome segreto nel `Create AstraControlCenter` campo del modulo.

1. Creare uno spazio dei nomi per l'operatore Astra Control Center:

```
oc create ns [netapp-acc-operator or custom namespace]
```

2. Creare un segreto in questo namespace:

```
oc create secret docker-registry astra-registry-cred n [netapp-acc-
operator or custom namespace] --docker-server=[your_registry_path]
--docker username=[username] --docker-password=[token]
```

> Astra Control supporta solo i segreti del Registro di sistema di Docker.

3. Completare i campi rimanenti in Il campo Create AstraControlCenter Form (Crea modulo AstraControlCenter).

Cosa succederà

Completare il "fasi rimanenti" Per verificare che Astra Control Center sia stato installato correttamente, configurare un controller di ingresso (opzionale) e accedere all'interfaccia utente. Inoltre, è necessario eseguire le operazioni "attività di installazione" al termine dell'installazione.

Installare il centro di controllo Astra con un backend di storage Cloud Volumes ONTAP

Con Astra Control Center, puoi gestire le tue app in un ambiente di cloud ibrido con cluster Kubernetes e istanze di Cloud Volumes ONTAP autogestiti. Puoi implementare Astra Control Center nei tuoi cluster Kubernetes on-premise o in uno dei cluster Kubernetes autogestiti nell'ambiente cloud.

Con una di queste implementazioni, è possibile eseguire operazioni di gestione dei dati delle applicazioni utilizzando Cloud Volumes ONTAP come back-end dello storage. È inoltre possibile configurare un bucket S3 come destinazione del backup.

Per installare Astra Control Center in Amazon Web Services (AWS), Google Cloud Platform (GCP) e Microsoft Azure con un backend di storage Cloud Volumes ONTAP, eseguire i seguenti passaggi a seconda dell'ambiente cloud in uso.

- Implementare Astra Control Center in Amazon Web Services
- Implementare Astra Control Center nella piattaforma Google Cloud
- Implementare Astra Control Center in Microsoft Azure

Puoi gestire le tue applicazioni nelle distribuzioni con cluster Kubernetes autogestiti, come OpenShift Container Platform (OCP). Solo i cluster OCP autogestiti sono validati per l'implementazione di Astra Control

Center.

Implementare Astra Control Center in Amazon Web Services

Puoi implementare Astra Control Center su un cluster Kubernetes autogestito ospitato su un cloud pubblico Amazon Web Services (AWS).

Ciò di cui hai bisogno per AWS

Prima di implementare Astra Control Center in AWS, sono necessari i seguenti elementi:

- Licenza Astra Control Center. Fare riferimento a. "Requisiti di licenza di Astra Control Center".
- "Soddisfare i requisiti di Astra Control Center".
- Account NetApp Cloud Central
- Se si utilizza OCP, autorizzazioni Red Hat OpenShift Container Platform (OCP) (a livello di spazio dei nomi per creare i pod)
- Credenziali AWS, Access ID e Secret Key con autorizzazioni che consentono di creare bucket e connettori
- Accesso e login al Registro dei container elastici (ECR) dell'account AWS
- Per accedere all'interfaccia utente di Astra Control è richiesta la zona ospitata di AWS e la voce Amazon Route 53

Requisiti dell'ambiente operativo per AWS

Astra Control Center richiede il seguente ambiente operativo per AWS:

- Red Hat OpenShift Container Platform dalla versione 4.11 alla 4.13

> Assicurarsi che l'ambiente operativo scelto per ospitare Astra Control Center soddisfi i requisiti delle risorse di base descritti nella documentazione ufficiale dell'ambiente.

Astra Control Center richiede le seguenti risorse oltre ai requisiti delle risorse dell'ambiente:

Componente	Requisito
Capacità di storage NetApp Cloud Volumes ONTAP di back-end	Almeno 300 GB disponibili
Nodi di lavoro (requisito AWS EC2)	Almeno 3 nodi di lavoro in totale, con 4 core vCPU e 12 GB di RAM ciascuno
Bilanciamento del carico	Tipo di servizio "LoadBalancer" disponibile per il traffico in ingresso da inviare ai servizi nel cluster dell'ambiente operativo
FQDN	Metodo per indirizzare l'FQDN di Astra Control Center all'indirizzo IP con bilanciamento del carico
Astra Trident (installato come parte del rilevamento dei cluster Kubernetes in NetApp BlueXP, in precedenza Cloud Manager)	Astra Trident 23,01 o versione successiva installato e configurato e NetApp ONTAP versione 9.9.1 o successiva come backend dello storage

Componente	Requisito
Registro delle immagini	NetApp fornisce un registro che è possibile utilizzare per ottenere le immagini di build di Astra Control Center: http://netappdownloads.jfrog.io/docker-astra-control-prod Contattare il supporto NetApp per ottenere istruzioni sull'utilizzo di questo registro di immagini durante il processo di installazione del centro di controllo Astra. Se non si riesce ad accedere al registro delle immagini di NetApp, è necessario disporre di un registro privato, ad esempio ECR (Elastic Container Registry) AWS, in cui è possibile trasferire le immagini di build di Astra Control Center. È necessario fornire l'URL del registro delle immagini in cui verranno caricate le immagini. Il cluster ospitato da Astra Control Center e il cluster gestito devono avere accesso alla stessa immagine di registro per poter eseguire il backup e il ripristino delle applicazioni utilizzando l'immagine basata su Restic.
Configurazione di Astra Trident/ONTAP	Astra Control Center richiede la creazione e l'impostazione di una classe di storage come classe di storage predefinita. Il centro di controllo Astra supporta le seguenti classi di storage Kubernetes create quando si importa il cluster Kubernetes in ONTAP BlueXP (in precedenza Cloud Manager). Questi sono forniti da Astra Trident: • `vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-ha-san csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-san csi.trident.netapp.io`

Questi requisiti presuppongono che Astra Control Center sia l'unica applicazione in esecuzione nell'ambiente operativo. Se nell'ambiente sono in esecuzione applicazioni aggiuntive, modificare di conseguenza questi requisiti minimi.

Il token del Registro di sistema AWS scade tra 12 ore, dopodiché sarà necessario rinnovare il segreto del Registro di sistema dell'immagine Docker.

Panoramica dell'implementazione per AWS

Di seguito viene fornita una panoramica del processo di installazione di Astra Control Center per AWS con Cloud Volumes ONTAP come backend di storage.

Ciascuna di queste fasi viene illustrata più dettagliatamente di seguito.

1. Assicurarsi di disporre di autorizzazioni IAM sufficienti.
2. Installare un cluster RedHat OpenShift su AWS.
3. Configurare AWS.
4. Configurare NetApp BlueXP per AWS.
5. Installare Astra Control Center per AWS.

Assicurarsi di disporre di autorizzazioni IAM sufficienti

Assicurarsi di disporre di ruoli e autorizzazioni IAM sufficienti per installare un cluster RedHat OpenShift e un connettore NetApp BlueXP (in precedenza Cloud Manager).

Vedere "Credenziali AWS iniziali".

Installare un cluster RedHat OpenShift su AWS

Installare un cluster RedHat OpenShift Container Platform su AWS.

Per istruzioni sull'installazione, vedere "Installazione di un cluster su AWS in OpenShift Container Platform".

Configurare AWS

Quindi, configurare AWS per creare una rete virtuale, configurare istanze di calcolo EC2 e creare un bucket AWS S3. Se non è possibile accedere a. Registro delle immagini del centro di controllo Astra di NetApp, Sarà inoltre necessario creare un Elastic Container Registry (ECR) per ospitare le immagini di Astra Control Center e inviare le immagini a questo registro.

Seguire la documentazione di AWS per completare i seguenti passaggi. Vedere "Documentazione di installazione di AWS".

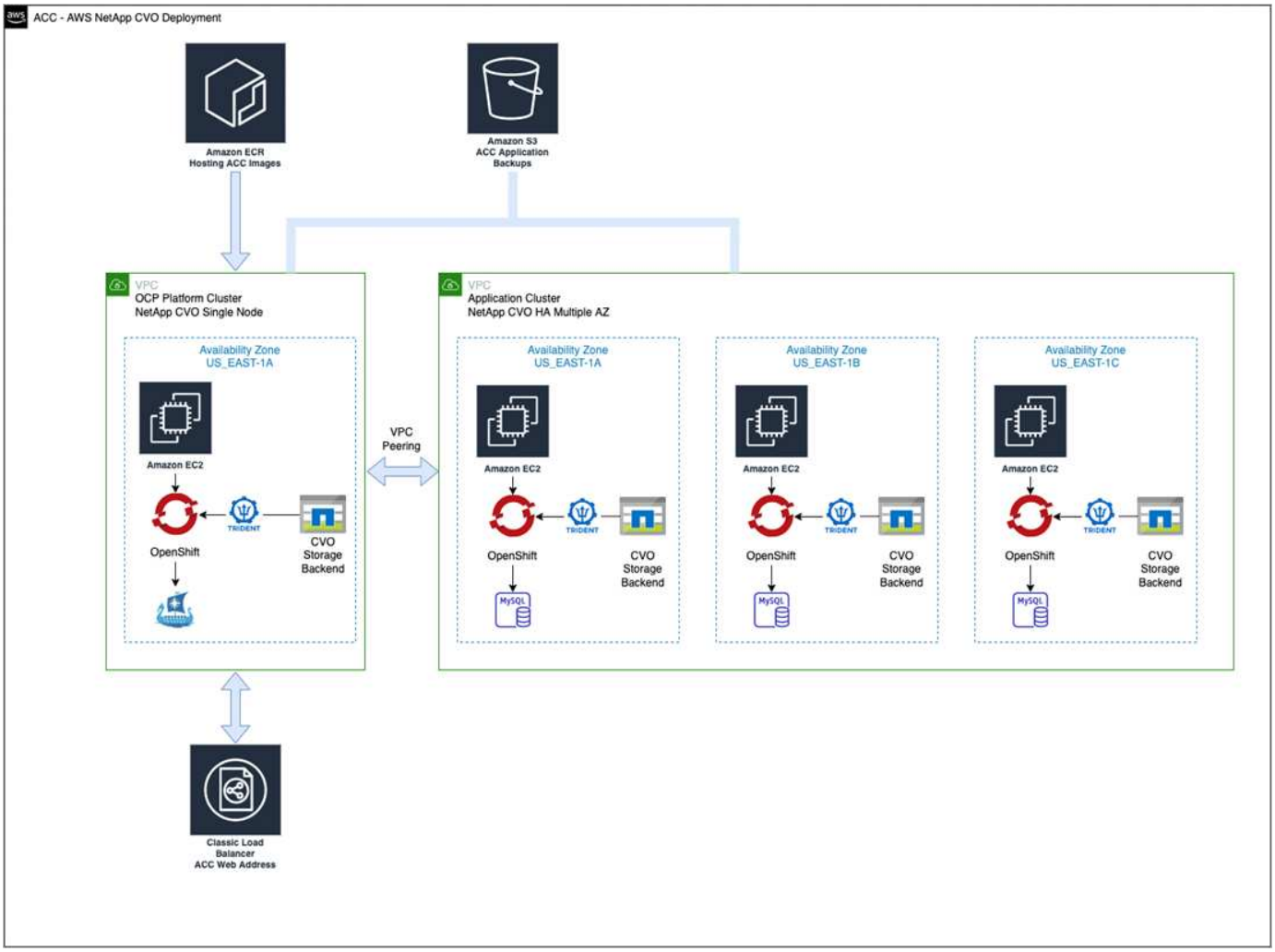
1. Creare una rete virtuale AWS.
2. Esaminare le istanze di calcolo EC2. Può trattarsi di un server bare metal o di macchine virtuali in AWS.
3. Se il tipo di istanza non corrisponde già ai requisiti minimi di risorsa Astra per i nodi master e worker, modificare il tipo di istanza in AWS per soddisfare i requisiti Astra. Fare riferimento a. "Requisiti di Astra Control Center".
4. Creare almeno un bucket AWS S3 per memorizzare i backup.
5. (Facoltativo) se non è possibile accedere a. Registro delle immagini di NetApp, effettuare le seguenti operazioni:
   a. Creare un AWS Elastic Container Registry (ECR) per ospitare tutte le immagini di Astra Control Center.

      Se non si crea ECR, il centro di controllo Astra non può accedere ai dati di monitoraggio da un cluster contenente Cloud Volumes ONTAP con un backend AWS. Il problema si verifica quando il cluster che si tenta di rilevare e gestire utilizzando Astra Control Center non dispone dell'accesso ad AWS ECR.

   b. Trasferire le immagini di Astra Control Center nel registro definito.

Il token AWS Elastic Container Registry (ECR) scade dopo 12 ore e causa il fallimento delle operazioni di cloni tra cluster. Questo problema si verifica quando si gestisce un backend di storage da Cloud Volumes ONTAP configurato per AWS. Per correggere questo problema, autenticare nuovamente con ECR e generare un nuovo segreto per la ripresa delle operazioni di clonazione.

Ecco un esempio di implementazione di AWS:



Configurare NetApp BlueXP per AWS

Utilizzando NetApp BlueXP (in precedenza Cloud Manager), creare uno spazio di lavoro, aggiungere un connettore ad AWS, creare un ambiente di lavoro e importare il cluster.

Seguire la documentazione di BlueXP per completare i seguenti passaggi. Vedere quanto segue:

- "Introduzione a Cloud Volumes ONTAP in AWS".
- "Creare un connettore in AWS utilizzando BlueXP"

Fasi

1. Aggiungi le tue credenziali a BlueXP.
2. Creare un'area di lavoro.

3. Aggiungere un connettore per AWS. Scegliere AWS come provider.
4. Crea un ambiente di lavoro per il tuo ambiente cloud.
   a. Location: "Amazon Web Services (AWS)"
   b. Tipo: "Cloud Volumes ONTAP ha"
5. Importare il cluster OpenShift. Il cluster si connetterà all'ambiente di lavoro appena creato.
   a. Per visualizzare i dettagli del cluster NetApp, selezionare **K8s** > **elenco cluster** > **Dettagli cluster**.
   b. Nell'angolo in alto a destra, prendere nota della versione di Astra Trident.
   c. Si noti che le classi di storage cluster Cloud Volumes ONTAP mostrano NetApp come provider.

      In questo modo, il cluster Red Hat OpenShift viene importato e viene assegnata una classe di storage predefinita. Selezionare la classe di storage.
      Astra Trident viene installato automaticamente come parte del processo di importazione e rilevamento.
6. Tenere presenti tutti i volumi e i volumi persistenti in questa implementazione di Cloud Volumes ONTAP.

Cloud Volumes ONTAP può funzionare come nodo singolo o in alta disponibilità. Se ha è attivato, annotare lo stato ha e lo stato di implementazione del nodo in esecuzione in AWS.

Installare Astra Control Center per AWS

Seguire lo standard "Istruzioni di installazione di Astra Control Center".

AWS utilizza il tipo di bucket S3 generico.

Implementare Astra Control Center nella piattaforma Google Cloud

Puoi implementare Astra Control Center su un cluster Kubernetes autogestito ospitato su un cloud pubblico Google Cloud Platform (GCP).

Cosa ti serve per GCP

Prima di implementare Astra Control Center in GCP, sono necessari i seguenti elementi:

- Licenza Astra Control Center. Fare riferimento a. "Requisiti di licenza di Astra Control Center".
- "Soddisfare i requisiti di Astra Control Center".
- Account NetApp Cloud Central
- Se si utilizza OCP, Red Hat OpenShift Container Platform (OCP) da 4.11 a 4.13
- Se si utilizza OCP, autorizzazioni Red Hat OpenShift Container Platform (OCP) (a livello di spazio dei nomi per creare i pod)
- GCP Service account con autorizzazioni che consentono di creare bucket e connettori

Requisiti dell'ambiente operativo per GCP

Assicurarsi che l'ambiente operativo scelto per ospitare Astra Control Center soddisfi i requisiti delle risorse di base descritti nella documentazione ufficiale dell'ambiente.

Astra Control Center richiede le seguenti risorse oltre ai requisiti delle risorse dell'ambiente:

Componente	Requisito
Capacità di storage NetApp Cloud Volumes ONTAP di back-end	Almeno 300 GB disponibili
Nodi di lavoro (requisito di calcolo GCP)	Almeno 3 nodi di lavoro in totale, con 4 core vCPU e 12 GB di RAM ciascuno
Bilanciamento del carico	Tipo di servizio "LoadBalancer" disponibile per il traffico in ingresso da inviare ai servizi nel cluster dell'ambiente operativo
FQDN (GCP DNS ZONE)	Metodo per indirizzare l'FQDN di Astra Control Center all'indirizzo IP con bilanciamento del carico
Astra Trident (installato come parte del rilevamento dei cluster Kubernetes in NetApp BlueXP, in precedenza Cloud Manager)	Astra Trident 23,01 o versione successiva installato e configurato e NetApp ONTAP versione 9.9.1 o successiva come backend dello storage
Registro delle immagini	NetApp fornisce un registro che è possibile utilizzare per ottenere le immagini di build di Astra Control Center: `http://netappdownloads.jfrog.io/docker-astra-control-prod` Contattare il supporto NetApp per ottenere istruzioni sull'utilizzo di questo registro di immagini durante il processo di installazione del centro di controllo Astra. Se non si riesce ad accedere al registro delle immagini di NetApp, è necessario disporre di un registro privato esistente, ad esempio il registro dei container di Google, in cui è possibile trasferire le immagini di creazione di Astra Control Center. È necessario fornire l'URL del registro delle immagini in cui verranno caricate le immagini. È necessario abilitare l'accesso anonimo per estrarre le immagini Restic per i backup.

Componente	Requisito
Configurazione di Astra Trident/ONTAP	Astra Control Center richiede la creazione e l'impostazione di una classe di storage come classe di storage predefinita. Il centro di controllo Astra supporta le seguenti classi di storage Kubernetes di ONTAP create quando si importa il cluster Kubernetes in NetApp BlueXP. Questi sono forniti da Astra Trident: • `vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-ha-san csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-san csi.trident.netapp.io`

Questi requisiti presuppongono che Astra Control Center sia l'unica applicazione in esecuzione nell'ambiente operativo. Se nell'ambiente sono in esecuzione applicazioni aggiuntive, modificare di conseguenza questi requisiti minimi.

Panoramica dell'implementazione per GCP

Di seguito viene fornita una panoramica del processo di installazione di Astra Control Center su un cluster OCP autogestiti in GCP con Cloud Volumes ONTAP come backend di storage.

Ciascuna di queste fasi viene illustrata più dettagliatamente di seguito.

1. Installare un cluster RedHat OpenShift su GCP.
2. Crea un progetto GCP e un cloud privato virtuale.
3. Assicurarsi di disporre di autorizzazioni IAM sufficienti.
4. Configurare GCP.
5. Configurare NetApp BlueXP per GCP.
6. Installare Astra Control Center per GCP.

Installare un cluster RedHat OpenShift su GCP

Il primo passo consiste nell'installare un cluster RedHat OpenShift su GCP.

Per istruzioni sull'installazione, consultare quanto segue:

- "Installazione di un cluster OpenShift in GCP"
- "Creazione di un account di servizio GCP"

Crea un progetto GCP e un cloud privato virtuale

Creare almeno un progetto GCP e Virtual Private Cloud (VPC).

OpenShift potrebbe creare i propri gruppi di risorse. Inoltre, è necessario definire un VPC GCP. Fare riferimento alla documentazione di OpenShift.

È possibile creare un gruppo di risorse del cluster di piattaforme e un gruppo di risorse del cluster OpenShift dell'applicazione di destinazione.

Assicurarsi di disporre di autorizzazioni IAM sufficienti

Assicurarsi di disporre di ruoli e autorizzazioni IAM sufficienti per installare un cluster RedHat OpenShift e un connettore NetApp BlueXP (in precedenza Cloud Manager).

Vedere "Credenziali e permessi GCP iniziali".

Configurare GCP

Quindi, configurare GCP per creare un VPC, configurare istanze di calcolo e creare un Google Cloud Object Storage. Se non è possibile accedere a. Registro delle immagini del centro di controllo Astra di NetApp, Sarà inoltre necessario creare un Google Container Registry per ospitare le immagini di Astra Control Center e inviare le immagini a questo registro.

Seguire la documentazione GCP per completare i seguenti passaggi. Vedere Installazione del cluster OpenShift in GCP.

1. Creare un progetto GCP e un VPC nel GCP che si intende utilizzare per il cluster OCP con backend CVO.
2. Esaminare le istanze di calcolo. Questo può essere un server bare metal o VM in GCP.
3. Se il tipo di istanza non corrisponde già ai requisiti minimi di risorsa Astra per i nodi master e worker, modificare il tipo di istanza in GCP per soddisfare i requisiti Astra. Fare riferimento a. "Requisiti di Astra Control Center".
4. Crea almeno un bucket di storage cloud GCP per memorizzare i tuoi backup.
5. Creare un segreto, necessario per l'accesso al bucket.
6. (Facoltativo) se non è possibile accedere a. Registro delle immagini di NetApp, effettuare le seguenti operazioni:

    a. Creare un Google Container Registry per ospitare le immagini di Astra Control Center.

    b. Impostare l'accesso al Google Container Registry per il push/pull di Docker per tutte le immagini di Astra Control Center.

    Esempio: Le immagini di Astra Control Center possono essere inviate a questo registro inserendo il seguente script:

    ```
    gcloud auth activate-service-account <service account email address>
    --key-file=<GCP Service Account JSON file>
    ```

    Questo script richiede un file manifesto di Astra Control Center e la posizione del Google Image Registry. Esempio:

```
manifestfile=acc.manifest.bundle.yaml
GCP_CR_REGISTRY=<target GCP image registry>
ASTRA_REGISTRY=<source Astra Control Center image registry>

while IFS= read -r image; do
    echo "image: $ASTRA_REGISTRY/$image $GCP_CR_REGISTRY/$image"
    root_image=${image%:*}
    echo $root_image
    docker pull $ASTRA_REGISTRY/$image
    docker tag $ASTRA_REGISTRY/$image $GCP_CR_REGISTRY/$image
    docker push $GCP_CR_REGISTRY/$image
done < acc.manifest.bundle.yaml
```

7. Impostare le zone DNS.

Configurare NetApp BlueXP per GCP

Utilizzando NetApp BlueXP (in precedenza Cloud Manager), creare uno spazio di lavoro, aggiungere un connettore a GCP, creare un ambiente di lavoro e importare il cluster.

Seguire la documentazione di BlueXP per completare i seguenti passaggi. Vedere "Introduzione a Cloud Volumes ONTAP in GCP".

Prima di iniziare

- Accesso all'account di servizio GCP con i ruoli e le autorizzazioni IAM richiesti

Fasi

1. Aggiungi le tue credenziali a BlueXP. Vedere "Aggiunta di account GCP".
2. Aggiungere un connettore per GCP.
   a. Scegliere "GCP" come provider.
   b. Immettere le credenziali GCP. Vedere "Creazione di un connettore in GCP da BlueXP".
   c. Assicurarsi che il connettore sia in funzione e passare a tale connettore.
3. Crea un ambiente di lavoro per il tuo ambiente cloud.
   a. Location: Italy
   b. Tipo: "Cloud Volumes ONTAP ha"
4. Importare il cluster OpenShift. Il cluster si connetterà all'ambiente di lavoro appena creato.
   a. Per visualizzare i dettagli del cluster NetApp, selezionare **K8s** > **elenco cluster** > **Dettagli cluster**.
   b. Nell'angolo in alto a destra, prendere nota della versione di Trident.
   c. Si noti che le classi di storage del cluster Cloud Volumes ONTAP mostrano "NetApp" come provider.

      In questo modo, il cluster Red Hat OpenShift viene importato e viene assegnata una classe di storage predefinita. Selezionare la classe di storage.
      Astra Trident viene installato automaticamente come parte del processo di importazione e rilevamento.
5. Tenere presenti tutti i volumi e i volumi persistenti in questa implementazione di Cloud Volumes ONTAP.

Cloud Volumes ONTAP può operare come un singolo nodo o in alta disponibilità (ha). Se ha è attivato, annotare lo stato ha e lo stato di implementazione del nodo in esecuzione in GCP.

Installare Astra Control Center per GCP

Seguire lo standard "Istruzioni di installazione di Astra Control Center".

GCP utilizza il tipo di bucket S3 generico.

1. Generare il Docker Secret per estrarre le immagini per l'installazione di Astra Control Center:

```
kubectl create secret docker-registry <secret name> --docker
-server=<Registry location> --docker-username=_json_key --docker
-password="$(cat <GCP Service Account JSON file>)" --namespace=pcloud
```

Implementare Astra Control Center in Microsoft Azure

Puoi implementare Astra Control Center su un cluster Kubernetes autogestito ospitato su un cloud pubblico Microsoft Azure.

Ciò di cui hai bisogno per Azure

Prima di implementare Astra Control Center in Azure, sono necessari i seguenti elementi:

- Licenza Astra Control Center. Fare riferimento a. "Requisiti di licenza di Astra Control Center".
- "Soddisfare i requisiti di Astra Control Center".
- Account NetApp Cloud Central
- Se si utilizza OCP, Red Hat OpenShift Container Platform (OCP) da 4.11 a 4.13
- Se si utilizza OCP, autorizzazioni Red Hat OpenShift Container Platform (OCP) (a livello di spazio dei nomi per creare i pod)
- Credenziali Azure con autorizzazioni che consentono di creare bucket e connettori

Requisiti dell'ambiente operativo per Azure

Assicurarsi che l'ambiente operativo scelto per ospitare Astra Control Center soddisfi i requisiti delle risorse di base descritti nella documentazione ufficiale dell'ambiente.

Astra Control Center richiede le seguenti risorse oltre ai requisiti delle risorse dell'ambiente:

Fare riferimento a. "Requisiti dell'ambiente operativo di Astra Control Center".

Componente	Requisito
Capacità di storage NetApp Cloud Volumes ONTAP di back-end	Almeno 300 GB disponibili

Componente	Requisito
Nodi di lavoro (requisito di calcolo di Azure)	Almeno 3 nodi di lavoro in totale, con 4 core vCPU e 12 GB di RAM ciascuno
Bilanciamento del carico	Tipo di servizio "LoadBalancer" disponibile per il traffico in ingresso da inviare ai servizi nel cluster dell'ambiente operativo
FQDN (Azure DNS zone)	Metodo per indirizzare l'FQDN di Astra Control Center all'indirizzo IP con bilanciamento del carico
Astra Trident (installato come parte del rilevamento dei cluster Kubernetes in NetApp BlueXP)	Astra Trident 23,01 o versione successiva installato e configurato e NetApp ONTAP versione 9.9.1 o successiva verrà utilizzato come backend di storage
Registro delle immagini	NetApp fornisce un registro che è possibile utilizzare per ottenere le immagini di build di Astra Control Center: `http://netappdownloads.jfrog.io/docker-astra-control-prod` Contattare il supporto NetApp per ottenere istruzioni sull'utilizzo di questo registro di immagini durante il processo di installazione del centro di controllo Astra. Se non si riesce ad accedere al registro delle immagini di NetApp, è necessario disporre di un registro privato esistente, ad esempio ACR (Azure Container Registry), in cui è possibile trasferire le immagini di build di Astra Control Center. È necessario fornire l'URL del registro delle immagini in cui verranno caricate le immagini. ⓘ È necessario abilitare l'accesso anonimo per estrarre le immagini Restic per i backup.
Configurazione di Astra Trident/ONTAP	Astra Control Center richiede la creazione e l'impostazione di una classe di storage come classe di storage predefinita. Il centro di controllo Astra supporta le seguenti classi di storage Kubernetes di ONTAP create quando si importa il cluster Kubernetes in NetApp BlueXP. Questi sono forniti da Astra Trident: • `vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-ha-san csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-san csi.trident.netapp.io`

Questi requisiti presuppongono che Astra Control Center sia l'unica applicazione in esecuzione nell'ambiente operativo. Se nell'ambiente sono in esecuzione applicazioni aggiuntive, modificare di conseguenza questi requisiti minimi.

Panoramica dell'implementazione di Azure

Ecco una panoramica del processo di installazione di Astra Control Center per Azure.

Ciascuna di queste fasi viene illustrata più dettagliatamente di seguito.

1. Installare un cluster RedHat OpenShift su Azure.
2. Creare gruppi di risorse Azure.
3. Assicurarsi di disporre di autorizzazioni IAM sufficienti.
4. Configurare Azure.
5. Configurare NetApp BlueXP (in precedenza Cloud Manager) per Azure.
6. Installare e configurare Astra Control Center per Azure.

Installare un cluster RedHat OpenShift su Azure

Il primo passo consiste nell'installare un cluster RedHat OpenShift su Azure.

Per istruzioni sull'installazione, consultare quanto segue:

- "Installazione del cluster OpenShift su Azure".
- "Installazione di un account Azure".

Creare gruppi di risorse Azure

Creare almeno un gruppo di risorse Azure.

OpenShift potrebbe creare i propri gruppi di risorse. Oltre a questi, è necessario definire anche i gruppi di risorse di Azure. Fare riferimento alla documentazione di OpenShift.

È possibile creare un gruppo di risorse del cluster di piattaforme e un gruppo di risorse del cluster OpenShift dell'applicazione di destinazione.

Assicurarsi di disporre di autorizzazioni IAM sufficienti

Assicurarsi di disporre di ruoli e autorizzazioni IAM sufficienti per l'installazione di un cluster RedHat OpenShift e di un connettore NetApp BlueXP.

Vedere "Credenziali e permessi di Azure".

Configurare Azure

Quindi, configurare Azure per creare una rete virtuale, configurare istanze di calcolo e creare un container Azure Blob. Se non è possibile accedere a. Registro delle immagini del centro di controllo Astra di NetApp, Sarà inoltre necessario creare un Azure Container Registry (ACR) per ospitare le immagini di Astra Control Center e inviare le immagini a questo registro.

Seguire la documentazione di Azure per completare i seguenti passaggi. Vedere "Installazione del cluster

OpenShift su Azure".

1. Creare una rete virtuale Azure.
2. Esaminare le istanze di calcolo. Si tratta di un server bare metal o di macchine virtuali in Azure.
3. Se il tipo di istanza non corrisponde già ai requisiti minimi di risorsa Astra per i nodi master e worker, modificare il tipo di istanza in Azure per soddisfare i requisiti Astra. Fare riferimento a. "Requisiti di Astra Control Center".
4. Creare almeno un container Azure Blob per memorizzare i backup.
5. Creare un account storage. Per creare un container da utilizzare come bucket in Astra Control Center è necessario un account storage.
6. Creare un segreto, necessario per l'accesso al bucket.
7. (Facoltativo) se non è possibile accedere a. Registro delle immagini di NetApp, effettuare le seguenti operazioni:

   a. Creare un Azure Container Registry (ACR) per ospitare le immagini di Astra Control Center.
   b. Impostare l'accesso ACR per la funzione push/pull di Docker per tutte le immagini di Astra Control Center.
   c. Inviare le immagini di Astra Control Center a questo registro utilizzando il seguente script:

      ```
      az acr login -n <AZ ACR URL/Location>
      This script requires the Astra Control Center manifest file and your
      Azure ACR location.
      ```

      Esempio:

   ```
   manifestfile=acc.manifest.bundle.yaml
   AZ_ACR_REGISTRY=<target Azure ACR image registry>
   ASTRA_REGISTRY=<source Astra Control Center image registry>

   while IFS= read -r image; do
       echo "image: $ASTRA_REGISTRY/$image $AZ_ACR_REGISTRY/$image"
       root_image=${image%:*}
       echo $root_image
       docker pull $ASTRA_REGISTRY/$image
       docker tag $ASTRA_REGISTRY/$image $AZ_ACR_REGISTRY/$image
       docker push $AZ_ACR_REGISTRY/$image
   done < acc.manifest.bundle.yaml
   ```

8. Impostare le zone DNS.

Configurare NetApp BlueXP (in precedenza Cloud Manager) per Azure

Utilizzando BlueXP (in precedenza Cloud Manager), creare un'area di lavoro, aggiungere un connettore ad Azure, creare un ambiente di lavoro e importare il cluster.

Seguire la documentazione di BlueXP per completare i seguenti passaggi. Vedere "Introduzione a BlueXP in Azure".

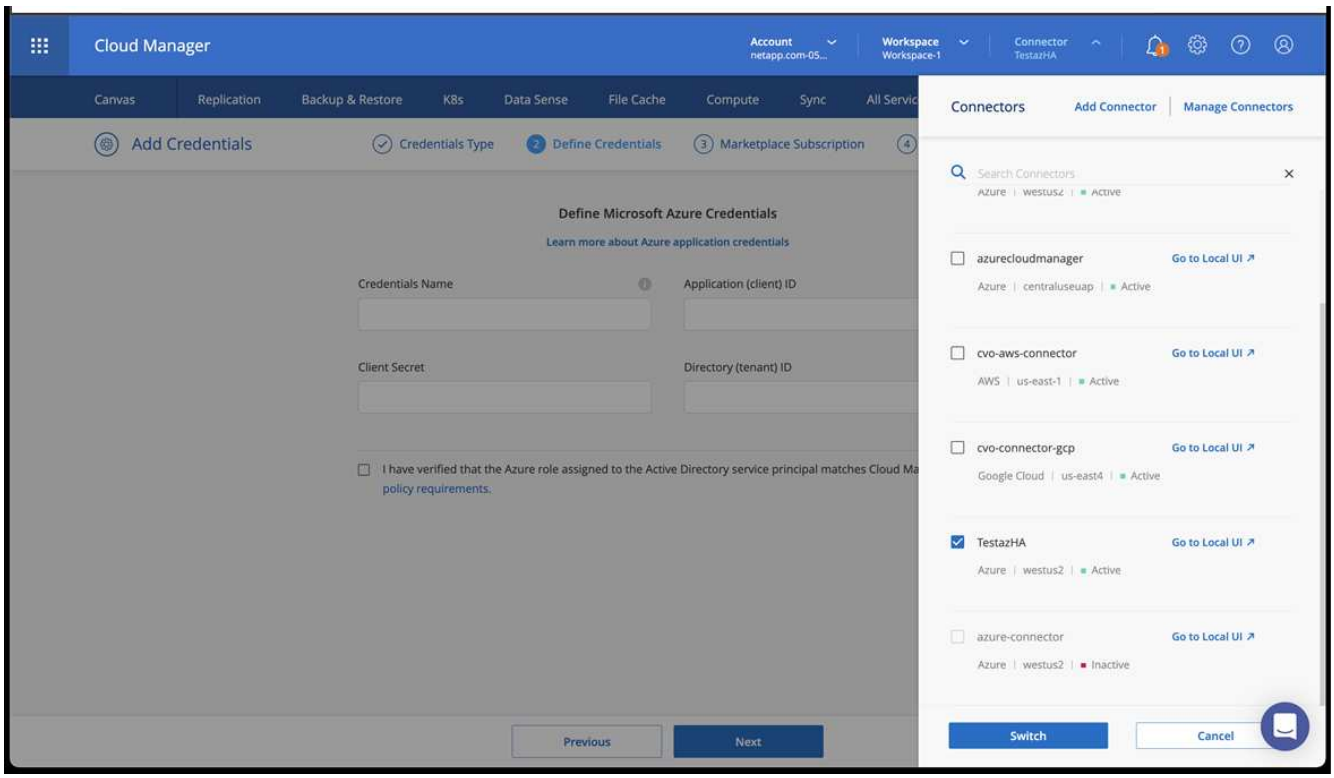
Prima di iniziare

Accesso all'account Azure con le autorizzazioni e i ruoli IAM richiesti

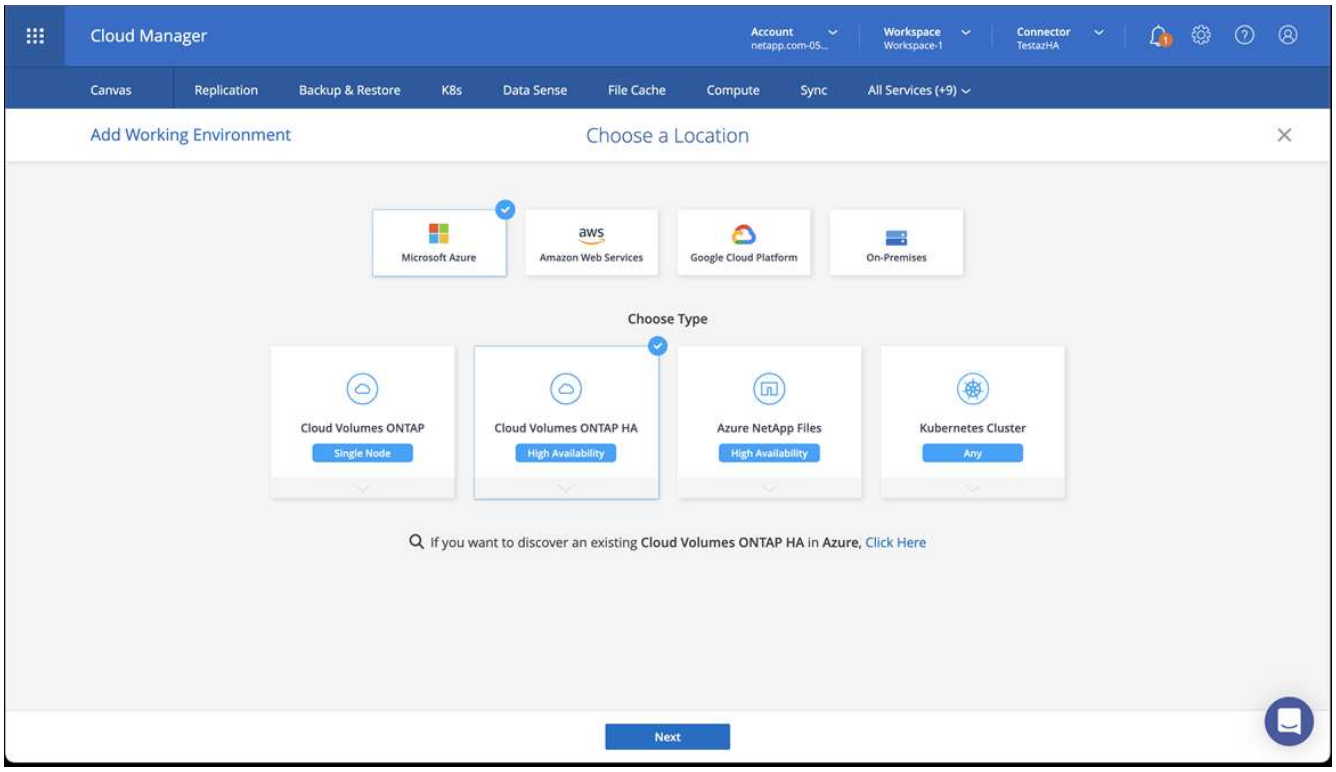
Fasi

1. Aggiungi le tue credenziali a BlueXP.
2. Aggiungere un connettore per Azure. Vedere "Policy BlueXP".
   a. Scegliere **Azure** come provider.
   b. Immettere le credenziali Azure, inclusi ID applicazione, segreto client e ID directory (tenant).

      Vedere "Creazione di un connettore in Azure da BlueXPr".
3. Assicurarsi che il connettore sia in funzione e passare a tale connettore.

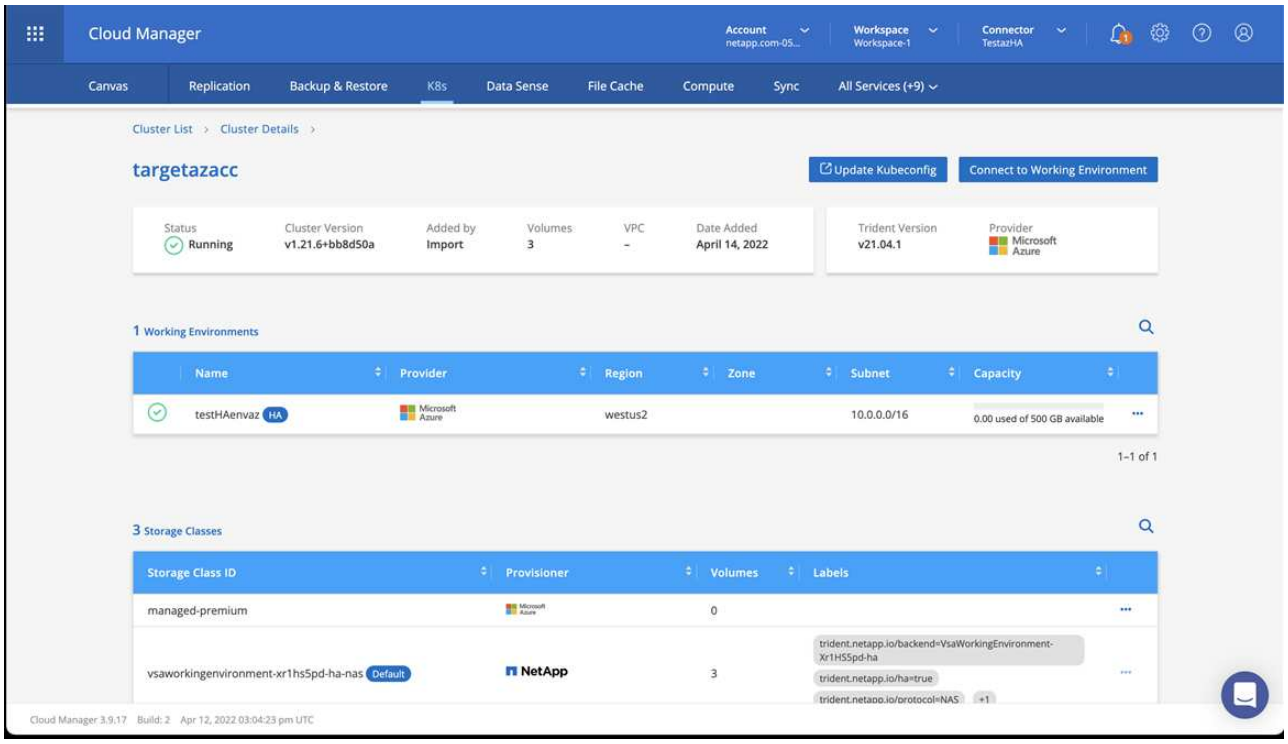


4. Crea un ambiente di lavoro per il tuo ambiente cloud.
   a. Percorso: "Microsoft Azure".
   b. Tipo: "Cloud Volumes ONTAP ha".



5. Importare il cluster OpenShift. Il cluster si connetterà all'ambiente di lavoro appena creato.

   a. Per visualizzare i dettagli del cluster NetApp, selezionare **K8s** > **elenco cluster** > **Dettagli cluster**.



   b. Nell'angolo in alto a destra, prendere nota della versione di Astra Trident.

   c. Si noti che le classi di storage cluster Cloud Volumes ONTAP mostrano NetApp come provider.

In questo modo viene importato il cluster Red Hat OpenShift e viene assegnata una classe di storage predefinita. Selezionare la classe di storage.

Astra Trident viene installato automaticamente come parte del processo di importazione e rilevamento.

6. Tenere presenti tutti i volumi e i volumi persistenti in questa implementazione di Cloud Volumes ONTAP.
7. Cloud Volumes ONTAP può funzionare come nodo singolo o in alta disponibilità. Se ha è attivato, annotare lo stato ha e lo stato di implementazione del nodo in esecuzione in Azure.

Installare e configurare Astra Control Center per Azure

Installare Astra Control Center con lo standard "istruzioni per l'installazione".

Utilizzando Astra Control Center, aggiungere un bucket Azure. Fare riferimento a. "Configurare Astra Control Center e aggiungere i bucket".

Configurare Astra Control Center dopo l'installazione

A seconda dell'ambiente in uso, potrebbe essere necessaria una configurazione aggiuntiva dopo l'installazione di Astra Control Center.

Rimuovere le limitazioni delle risorse

Alcuni ambienti utilizzano gli oggetti ResourceQuotas e LimitRanges per impedire alle risorse di uno spazio dei nomi di consumare tutta la CPU e la memoria disponibili nel cluster. Astra Control Center non imposta limiti massimi, pertanto non sarà conforme a tali risorse. Se l'ambiente è configurato in questo modo, è necessario rimuovere tali risorse dagli spazi dei nomi in cui si intende installare Astra Control Center.

Per recuperare e rimuovere le quote e i limiti, procedere come segue. In questi esempi, l'output del comando viene visualizzato immediatamente dopo il comando.

Fasi

1. Ottenere le quote delle risorse in `netapp-acc` namespace (o personalizzato):

```
kubectl get quota -n [netapp-acc or custom namespace]
```

Risposta:

```
NAME          AGE   REQUEST                                              LIMIT
pods-high     16s   requests.cpu: 0/20, requests.memory: 0/100Gi
limits.cpu: 0/200, limits.memory: 0/1000Gi
pods-low      15s   requests.cpu: 0/1, requests.memory: 0/1Gi
limits.cpu: 0/2, limits.memory: 0/2Gi
pods-medium   16s   requests.cpu: 0/10, requests.memory: 0/20Gi
limits.cpu: 0/20, limits.memory: 0/200Gi
```

2. Eliminare tutte le quote delle risorse in base al nome:

```
kubectl delete resourcequota pods-high -n [netapp-acc or custom
namespace]
```

```
kubectl delete resourcequota pods-low -n [netapp-acc or custom
namespace]
```

```
kubectl delete resourcequota pods-medium -n [netapp-acc or custom
namespace]
```

3. Ottenere gli intervalli di limite in `netapp-acc` namespace (o personalizzato):

```
kubectl get limits -n [netapp-acc or custom namespace]
```

Risposta:

```
NAME              CREATED AT
cpu-limit-range   2022-06-27T19:01:23Z
```

4. Eliminare gli intervalli di limiti in base al nome:

```
kubectl delete limitrange cpu-limit-range -n [netapp-acc or custom
namespace]
```

Aggiungere un certificato TLS personalizzato

Astra Control Center utilizza per impostazione predefinita un certificato TLS autofirmato per il traffico dei controller di ingresso (solo in alcune configurazioni) e l'autenticazione dell'interfaccia utente Web con i browser Web. È possibile rimuovere il certificato TLS autofirmato esistente e sostituirlo con un certificato TLS firmato da un'autorità di certificazione (CA).

Il certificato autofirmato predefinito viene utilizzato per due tipi di connessione:

- Connessioni HTTPS all'interfaccia utente Web di Astra Control Center
- Traffico del controller di ingresso (solo se `ingressType: "AccTraefik"` la proprietà è stata impostata in `astra_control_center.yaml` Durante l'installazione di Astra Control Center)

La sostituzione del certificato TLS predefinito sostituisce il certificato utilizzato per l'autenticazione di queste connessioni.

Prima di iniziare

- Kubernetes cluster con Astra Control Center installato
- Accesso amministrativo a una shell dei comandi sul cluster da eseguire `kubectl` comandi
- Chiave privata e file di certificato dalla CA

Rimuovere il certificato autofirmato

Rimuovere il certificato TLS autofirmato esistente.

1. Utilizzando SSH, accedere al cluster Kubernetes che ospita Astra Control Center come utente amministrativo.
2. Individuare il segreto TLS associato al certificato corrente utilizzando il seguente comando, sostituendo `<ACC-deployment-namespace>` Con lo spazio dei nomi di implementazione di Astra Control Center:

```
kubectl get certificate -n <ACC-deployment-namespace>
```

3. Eliminare il certificato e il segreto attualmente installati utilizzando i seguenti comandi:

```
kubectl delete cert cert-manager-certificates -n <ACC-deployment-
namespace>
```

```
kubectl delete secret secure-testing-cert -n <ACC-deployment-namespace>
```

Aggiungere un nuovo certificato utilizzando la riga di comando

Aggiungere un nuovo certificato TLS firmato da una CA.

1. Utilizzare il seguente comando per creare il nuovo segreto TLS con la chiave privata e i file di certificato della CA, sostituendo gli argomenti tra parentesi <> con le informazioni appropriate:

```
kubectl create secret tls <secret-name> --key <private-key-filename>
--cert <certificate-filename> -n <ACC-deployment-namespace>
```

2. Utilizzare il seguente comando e l'esempio per modificare il file CRD (Custom Resource Definition) del cluster e modificare `spec.selfSigned` valore a. `spec.ca.secretName` Per fare riferimento al segreto TLS creato in precedenza:

```
kubectl edit clusterissuers.cert-manager.io/cert-manager-certificates -n
<ACC-deployment-namespace>
```

   CRD:

```
#spec:
#  selfSigned: {}

spec:
  ca:
    secretName: <secret-name>
```

3. Utilizzare il seguente comando e l'output di esempio per confermare che le modifiche sono corrette e che il cluster è pronto per validare i certificati, sostituendo `<ACC-deployment-namespace>` Con lo spazio dei nomi di implementazione di Astra Control Center:

```
kubectl describe clusterissuers.cert-manager.io/cert-manager-
certificates -n <ACC-deployment-namespace>
```

Risposta:

```
Status:
  Conditions:
    Last Transition Time:  2021-07-01T23:50:27Z
    Message:               Signing CA verified
    Reason:                KeyPairVerified
    Status:                True
    Type:                  Ready
Events:                    <none>
```

4. Creare il `certificate.yaml` file utilizzando il seguente esempio, sostituendo i valori segnaposto tra parentesi <> con le informazioni appropriate:

```
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  <strong>name: <certificate-name></strong>
  namespace: <ACC-deployment-namespace>
spec:
  <strong>secretName: <certificate-secret-name></strong>
  duration: 2160h # 90d
  renewBefore: 360h # 15d
  dnsNames:
  <strong>- <astra.dnsname.example.com></strong> #Replace with the
correct Astra Control Center DNS address
  issuerRef:
    kind: ClusterIssuer
    name: cert-manager-certificates
```

5. Creare il certificato utilizzando il seguente comando:

```
kubectl apply -f certificate.yaml
```

6. Utilizzando il seguente comando e l'output di esempio, verificare che il certificato sia stato creato correttamente e con gli argomenti specificati durante la creazione (ad esempio nome, durata, scadenza di rinnovo e nomi DNS).

```
kubectl describe certificate -n <ACC-deployment-namespace>
```

Risposta:

```
Spec:
  Dns Names:
    astra.example.com
  Duration:  125h0m0s
  Issuer Ref:
    Kind:        ClusterIssuer
    Name:        cert-manager-certificates
  Renew Before:  61h0m0s
  Secret Name:   <certificate-secret-name>
Status:
  Conditions:
    Last Transition Time:  2021-07-02T00:45:41Z
    Message:               Certificate is up to date and has not expired
    Reason:                Ready
    Status:                True
    Type:                  Ready
  Not After:               2021-07-07T05:45:41Z
  Not Before:              2021-07-02T00:45:41Z
  Renewal Time:            2021-07-04T16:45:41Z
  Revision:                1
Events:                    <none>
```

7. Modificare il CRD degli archivi TLS in modo che punti al nuovo nome segreto del certificato utilizzando il seguente comando ed esempio, sostituendo i valori segnaposto tra parentesi <> con le informazioni appropriate

```
kubectl edit tlsstores.traefik.io -n <ACC-deployment-namespace>
```

CRD:

```
...
spec:
  defaultCertificate:
    secretName: <certificate-secret-name>
```

8. Modificare l'opzione TLS CRD di ingresso per indicare il nuovo segreto del certificato utilizzando il seguente comando ed esempio, sostituendo i valori segnaposto tra parentesi <> con le informazioni appropriate:

```
kubectl edit ingressroutes.traefik.io -n <ACC-deployment-namespace>
```

CRD:

```
...
 tls:
    secretName: <certificate-secret-name>
```

9. Utilizzando un browser Web, accedere all'indirizzo IP di implementazione di Astra Control Center.
10. Verificare che i dettagli del certificato corrispondano ai dettagli del certificato installato.
11. Esportare il certificato e importare il risultato nel gestore dei certificati nel browser Web.

Configurare Astra Control Center

Dopo aver installato Astra Control Center, aver effettuato l'accesso all'interfaccia utente e aver modificato la password, è necessario impostare una licenza, aggiungere cluster, abilitare l'autenticazione, gestire lo storage e aggiungere bucket.

Attività

- Aggiungere una licenza per Astra Control Center
- Prepara il tuo ambiente per la gestione dei cluster utilizzando Astra Control
- Aggiungere il cluster
- Abilitare l'autenticazione sul backend dello storage ONTAP
- Aggiungere un backend di storage
- Aggiungi un bucket

Aggiungere una licenza per Astra Control Center

Quando si installa Astra Control Center, è già installata una licenza di valutazione integrata. Se stai valutando Astra Control Center, puoi saltare questo passaggio.

È possibile aggiungere una nuova licenza utilizzando l'interfaccia utente di Astra Control o. "API di controllo Astra".

Le licenze di Astra Control Center misurano le risorse CPU utilizzando le unità CPU di Kubernetes e tengono conto delle risorse CPU assegnate ai nodi di lavoro di tutti i cluster Kubernetes gestiti. Le licenze si basano sull'utilizzo di vCPU. Per ulteriori informazioni sul calcolo delle licenze, fare riferimento a. "Licensing".

Se l'installazione supera il numero concesso in licenza di unità CPU, Astra Control Center impedisce la gestione di nuove applicazioni. Quando viene superata la capacità, viene visualizzato un avviso.

Per aggiornare una licenza di valutazione o una licenza completa, fare riferimento a. "Aggiornare una licenza esistente".

Prima di iniziare

- Accesso a un'istanza di Astra Control Center appena installata.
- Autorizzazioni per il ruolo di amministratore.
- R "File di licenza NetApp" (NLF).

Fasi

1. Accedere all'interfaccia utente di Astra Control Center.
2. Selezionare **account** > **licenza**.
3. Selezionare **Aggiungi licenza**.
4. Individuare il file di licenza (NLF) scaricato.
5. Selezionare **Aggiungi licenza**.

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

Se si dispone di una licenza di valutazione e non si inviano dati a AutoSupport, assicurarsi di memorizzare l'ID account per evitare la perdita di dati in caso di guasto del centro di controllo Astra.

Prepara il tuo ambiente per la gestione dei cluster utilizzando Astra Control

Prima di aggiungere un cluster, assicurarsi che siano soddisfatte le seguenti condizioni preliminari. È inoltre necessario eseguire controlli di idoneità per assicurarsi che il cluster sia pronto per essere aggiunto ad Astra Control Center e creare ruoli per la gestione del cluster.

Prima di iniziare

- **Soddisfare i requisiti ambientali**: L'ambiente soddisfa i requisiti "requisiti dell'ambiente operativo" Per Astra Trident e Astra Control Center.
- **Configura nodi di lavoro**: Assicurarsi di configurare i nodi di lavoro nel cluster con i driver di storage appropriati in modo che i pod possano interagire con lo storage backend.
- **Rendere accessibile kubeconfig**: Si ha accesso al "default cluster kubeconfig" quello "la configurazione è stata eseguita durante l'installazione".
- **Considerazioni sull'autorità di certificazione**: Se si aggiunge il cluster utilizzando un file kubeconfig che fa riferimento a un'autorità di certificazione (CA) privata, aggiungere la seguente riga al `cluster` sezione del file kubeconfig. In questo modo si permette ad Astra Control di aggiungere il cluster:

```
insecure-skip-tls-verify: true
```

- **Abilita restrizioni PSA**: Se il cluster ha abilitato l'applicazione di accesso di sicurezza pod, che è standard per i cluster Kubernetes 1,25 e versioni successive, è necessario abilitare le restrizioni PSA nei seguenti spazi dei nomi:
  - `netapp-acc-operator` spazio dei nomi:

```
kubectl label --overwrite ns netapp-acc-operator pod-
security.kubernetes.io/enforce=privileged
```

  - `netapp monitoring` spazio dei nomi:

```
kubectl label --overwrite ns netapp-monitoring pod-
security.kubernetes.io/enforce=privileged
```

- **Requisiti Astra Trident**:
  - **Installa una versione supportata**: Una versione di Astra Trident che è "Supportato da Astra Control Center" è installato:

    È possibile "Implementare Astra Trident" Utilizzando l'operatore Astra Trident (manualmente o utilizzando Helm Chart) o. `tridentctl`. Prima di installare o aggiornare Astra Trident, consultare "frontend, backend e configurazioni host supportati".

  - **Configurare un backend di storage Astra Trident**: Deve essere almeno un backend di storage Astra Trident "configurato" sul cluster.
  - **Configurare classi di storage Astra Trident**: Deve essere almeno una classe di storage Astra Trident "configurato" sul cluster. Se è configurata una classe di storage predefinita, assicurarsi che sia l'unica classe di storage con l'annotazione predefinita.
  - **Configurare un controller snapshot di volume Astra Trident e installare una classe snapshot di volume**: Il controller snapshot di volume deve essere "installato" In modo che le snapshot possano essere create in Astra Control. Almeno un tridente Astra `VolumeSnapshotClass` lo è stato "configurazione" da un amministratore.
- **Astra Control provisioner**: Per utilizzare funzionalità avanzate di gestione e provisioning dello storage di Astra Control Provivisioner accessibili solo agli utenti di Astra Control, devi installare Astra Trident 23,10 o versioni successive e abilitarlo "Funzionalità Astra Control Provisioner".
- **Credenziali ONTAP**: Per eseguire il backup e il ripristino delle applicazioni con il centro di controllo Astra sono necessarie le credenziali ONTAP e un ID utente e un superutente impostati sul sistema ONTAP di backup.

  Eseguire i seguenti comandi nella riga di comando di ONTAP:

```
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -superuser sys
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -anon 65534
```

- **Solo Rancher**: Quando si gestiscono i cluster di applicazioni in un ambiente Rancher, modificare il contesto predefinito del cluster di applicazioni nel file kubeconfig fornito da Rancher per utilizzare un contesto del piano di controllo invece del contesto del server API Rancher. In questo modo si riduce il carico sul server API Rancher e si migliorano le performance.

Eseguire i controlli di idoneità

Eseguire i seguenti controlli di idoneità per assicurarsi che il cluster sia pronto per essere aggiunto ad Astra Control Center.

Fasi

1. Controllare la versione di Astra Trident.

```
kubectl get tridentversions -n trident
```

Se Astra Trident esiste, l'output è simile a quanto segue:

```
NAME      VERSION
trident   23.XX.X
```

Se Astra Trident non esiste, viene visualizzato un output simile al seguente:

```
error: the server doesn't have a resource type "tridentversions"
```

> Se Astra Trident non è installato o se la versione installata non è la più recente, è necessario installare l'ultima versione di Astra Trident prima di procedere. Fare riferimento a. "Documentazione di Astra Trident" per istruzioni.

2. Assicurarsi che i pod siano in funzione:

```
kubectl get pods -n trident
```

3. Determinare se le classi di storage utilizzano i driver Astra Trident supportati. Il nome del provider deve essere `csi.trident.netapp.io`. Vedere il seguente esempio:

```
kubectl get sc
```

Esempio di risposta:

```
NAME                    PROVISIONER             RECLAIMPOLICY
VOLUMEBINDINGMODE  ALLOWVOLUMEEXPANSION  AGE
ontap-gold (default)  csi.trident.netapp.io  Delete          Immediate
true                   5d23h
```

Creare un ruolo cluster kubeconfig

È possibile, in via opzionale, creare un ruolo di amministratore con autorizzazioni limitate o estese per Astra Control Center. Questa procedura non è necessaria per la configurazione di Astra Control Center, in quanto è già stata configurata una configurazione come parte di "processo di installazione".

Questa procedura consente di creare una configurazione separata se uno dei seguenti scenari si applica al proprio ambiente:

- Si desidera limitare le autorizzazioni di Astra Control sui cluster gestiti

- Si utilizzano più contesti e non è possibile utilizzare il kubeconfig di Astra Control predefinito configurato durante l'installazione oppure un ruolo limitato con un singolo contesto non funziona nell'ambiente

Prima di iniziare

Prima di completare la procedura, assicurarsi di disporre dei seguenti elementi per il cluster che si desidera gestire:

- kubectl v1.23 o versione successiva installata
- Accesso kubectl al cluster che si intende aggiungere e gestire con Astra Control Center

> Per questa procedura, non è necessario l'accesso kubectl al cluster che esegue Astra Control Center.

- Un kubeconfig attivo per il cluster che si intende gestire con i diritti di amministratore del cluster per il contesto attivo

Fasi

1. Creare un account di servizio:

   a. Creare un file di account del servizio denominato `astracontrol-service-account.yaml`.

      Regolare il nome e lo spazio dei nomi in base alle esigenze. Se le modifiche vengono apportate qui, è necessario applicare le stesse modifiche nei passaggi seguenti.

```
<strong>astracontrol-service-account.yaml</strong>
```

+

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: astracontrol-service-account
  namespace: default
```

   a. Applicare l'account del servizio:

```
kubectl apply -f astracontrol-service-account.yaml
```

2. Creare uno dei seguenti ruoli del cluster con autorizzazioni sufficienti per la gestione di un cluster da parte di Astra Control:

   - **Ruolo cluster limitato**: Questo ruolo contiene le autorizzazioni minime necessarie per la gestione di un cluster da parte di Astra Control:

Espandere per i passaggi

i. Creare un `ClusterRole` file chiamato, ad esempio, `astra-admin-account.yaml`.

Regolare il nome e lo spazio dei nomi in base alle esigenze. Se le modifiche vengono apportate qui, è necessario applicare le stesse modifiche nei passaggi seguenti.

```
<strong>astra-admin-account.yaml</strong>
```

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: astra-admin-account
rules:

# Get, List, Create, and Update all resources
# Necessary to backup and restore all resources in an app
- apiGroups:
  - '*'
  resources:
  - '*'
  verbs:
  - get
  - list
  - create
  - patch

# Delete Resources
# Necessary for in-place restore and AppMirror failover
- apiGroups:
  - ""
  - apps
  - autoscaling
  - batch
  - crd.projectcalico.org
  - extensions
  - networking.k8s.io
  - policy
  - rbac.authorization.k8s.io
  - snapshot.storage.k8s.io
  - trident.netapp.io
  resources:
  - configmaps
  - cronjobs
  - daemonsets
```

```
  - deployments
  - horizontalpodautoscalers
  - ingresses
  - jobs
  - namespaces
  - networkpolicies
  - persistentvolumeclaims
  - poddisruptionbudgets
  - pods
  - podtemplates
  - podsecuritypolicies
  - replicasets
  - replicationcontrollers
  - replicationcontrollers/scale
  - rolebindings
  - roles
  - secrets
  - serviceaccounts
  - services
  - statefulsets
  - tridentmirrorrelationships
  - tridentsnapshotinfos
  - volumesnapshots
  - volumesnapshotcontents
  verbs:
  - delete

# Watch resources
# Necessary to monitor progress
- apiGroups:
  - ""
  resources:
  - pods
  - replicationcontrollers
  - replicationcontrollers/scale
  verbs:
  - watch

# Update resources
- apiGroups:
  - ""
  - build.openshift.io
  - image.openshift.io
  resources:
  - builds/details
  - replicationcontrollers
```

```
  - replicationcontrollers/scale
  - imagestreams/layers
  - imagestreamtags
  - imagetags
  verbs:
  - update

# Use PodSecurityPolicies
- apiGroups:
  - extensions
  - policy
  resources:
  - podsecuritypolicies
  verbs:
  - use
```

ii. (Solo per i cluster OpenShift) aggiungere quanto segue alla fine di `astra-admin-account.yaml` o dopo `# Use PodSecurityPolicies` sezione:

```
# OpenShift security
- apiGroups:
  - security.openshift.io
  resources:
  - securitycontextconstraints
  verbs:
  - use
```

iii. Applicare il ruolo del cluster:

```
kubectl apply -f astra-admin-account.yaml
```

- **Ruolo cluster esteso**: Questo ruolo contiene autorizzazioni estese per un cluster che deve essere gestito da Astra Control. È possibile utilizzare questo ruolo se si utilizzano più contesti e non è possibile utilizzare il kubeconfig di Astra Control predefinito configurato durante l'installazione oppure se un ruolo limitato con un singolo contesto non funziona nell'ambiente:

> Quanto segue `ClusterRole` I passaggi sono un esempio generale di Kubernetes. Consultare la documentazione della distribuzione Kubernetes per istruzioni specifiche sull'ambiente in uso.

Espandere per i passaggi

i. Creare un `ClusterRole` file chiamato, ad esempio, `astra-admin-account.yaml`.

Regolare il nome e lo spazio dei nomi in base alle esigenze. Se le modifiche vengono apportate qui, è necessario applicare le stesse modifiche nei passaggi seguenti.

```
<strong>astra-admin-account.yaml</strong>
```

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: astra-admin-account
rules:
- apiGroups:
  - '*'
  resources:
  - '*'
  verbs:
  - '*'
- nonResourceURLs:
  - '*'
  verbs:
  - '*'
```

ii. Applicare il ruolo del cluster:

```
kubectl apply -f astra-admin-account.yaml
```

3. Creare l'associazione del ruolo del cluster all'account del servizio per il ruolo del cluster:

a. Creare un `ClusterRoleBinding` file chiamato `astracontrol-clusterrolebinding.yaml`.

Modificare i nomi e gli spazi dei nomi modificati quando si crea l'account del servizio, in base alle necessità.

```
<strong>astracontrol-clusterrolebinding.yaml</strong>
```

+

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: astracontrol-admin
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: astra-admin-account
subjects:
- kind: ServiceAccount
  name: astracontrol-service-account
  namespace: default
```

a. Applicare l'associazione del ruolo del cluster:

```
kubectl apply -f astracontrol-clusterrolebinding.yaml
```

4. Creare e applicare il token secret:

a. Creare un file token secret chiamato `secret-astracontrol-service-account.yaml`.

```
<strong>secret-astracontrol-service-account.yaml</strong>
```

```
apiVersion: v1
kind: Secret
metadata:
  name: secret-astracontrol-service-account
  namespace: default
  annotations:
    kubernetes.io/service-account.name: "astracontrol-service-
account"
type: kubernetes.io/service-account-token
```

b. Applicare il token secret:

```
kubectl apply -f secret-astracontrol-service-account.yaml
```

5. Aggiungere il token secret all'account del servizio aggiungendo il nome a `secrets` array (l'ultima riga dell'esempio seguente):

```
kubectl edit sa astracontrol-service-account
```

```
apiVersion: v1
imagePullSecrets:
- name: astracontrol-service-account-dockercfg-48xhx
kind: ServiceAccount
metadata:
  annotations:
    kubectl.kubernetes.io/last-applied-configuration: |

{"apiVersion":"v1","kind":"ServiceAccount","metadata":{"annotations":{},
"name":"astracontrol-service-account","namespace":"default"}}
  creationTimestamp: "2023-06-14T15:25:45Z"
  name: astracontrol-service-account
  namespace: default
  resourceVersion: "2767069"
  uid: 2ce068c4-810e-4a96-ada3-49cbf9ec3f89
secrets:
- name: astracontrol-service-account-dockercfg-48xhx
<strong>- name: secret-astracontrol-service-account</strong>
```

6. Elencare i segreti dell'account di servizio, sostituendo `<context>` con il contesto corretto per l'installazione:

```
kubectl get serviceaccount astracontrol-service-account --context
<context> --namespace default -o json
```

La fine dell'output dovrebbe essere simile a quanto segue:

```
"secrets": [
{ "name": "astracontrol-service-account-dockercfg-48xhx"},
{ "name": "secret-astracontrol-service-account"}
]
```

Gli indici di ciascun elemento in `secrets` l'array inizia con 0. Nell'esempio precedente, l'indice per `astracontrol-service-account-dockercfg-48xhx` sarebbe 0 e l'indice per `secret-astracontrol-service-account` sarebbe 1. Nell'output, annotare il numero dell'indice per il segreto dell'account del servizio. Questo numero di indice sarà necessario nella fase successiva.

7. Generare il kubeconfig come segue:
   a. Creare un `create-kubeconfig.sh` file. Sostituire `TOKEN_INDEX` all'inizio del seguente script con il valore corretto.

```
<strong>create-kubeconfig.sh</strong>
```

```
# Update these to match your environment.
# Replace TOKEN_INDEX with the correct value
# from the output in the previous step. If you
# didn't change anything else above, don't change
# anything else here.

SERVICE_ACCOUNT_NAME=astracontrol-service-account
NAMESPACE=default
NEW_CONTEXT=astracontrol
KUBECONFIG_FILE='kubeconfig-sa'

CONTEXT=$(kubectl config current-context)

SECRET_NAME=$(kubectl get serviceaccount ${SERVICE_ACCOUNT_NAME} \
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.secrets[TOKEN_INDEX].name}')
TOKEN_DATA=$(kubectl get secret ${SECRET_NAME} \
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.data.token}')

TOKEN=$(echo ${TOKEN_DATA} | base64 -d)

# Create dedicated kubeconfig
# Create a full copy
kubectl config view --raw > ${KUBECONFIG_FILE}.full.tmp

# Switch working context to correct context
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp config use-context
${CONTEXT}

# Minify
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp \
  config view --flatten --minify > ${KUBECONFIG_FILE}.tmp

# Rename context
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  rename-context ${CONTEXT} ${NEW_CONTEXT}

# Create token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-credentials ${CONTEXT}-${NAMESPACE}-token-user \
  --token ${TOKEN}

# Set context to use token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
```

```
  set-context ${NEW_CONTEXT} --user ${CONTEXT}-${NAMESPACE}-token
-user

# Set context to correct namespace
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --namespace ${NAMESPACE}

# Flatten/minify kubeconfig
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  view --flatten --minify > ${KUBECONFIG_FILE}

# Remove tmp
rm ${KUBECONFIG_FILE}.full.tmp
rm ${KUBECONFIG_FILE}.tmp
```

b. Eseguire la sorgente dei comandi per applicarli al cluster Kubernetes.

```
source create-kubeconfig.sh
```

8. (Facoltativo) rinominare il kubeconfig con un nome significativo per il cluster.

```
mv kubeconfig-sa YOUR_CLUSTER_NAME_kubeconfig
```

Quali sono le prossime novità?

Dopo aver verificato che i prerequisiti sono stati soddisfatti, sei pronto aggiungere un cluster.

Aggiungere il cluster

Per iniziare a gestire le tue applicazioni, Aggiungi un cluster Kubernetes e gestilo come risorsa di calcolo. Devi aggiungere un cluster per Astra Control Center per scoprire le tue applicazioni Kubernetes.

Si consiglia ad Astra Control Center di gestire il cluster su cui viene implementato prima di aggiungere altri cluster ad Astra Control Center da gestire. La gestione del cluster iniziale è necessaria per inviare i dati Kublemetrics e i dati associati al cluster per metriche e troubleshooting.

Prima di iniziare

- Prima di aggiungere un cluster, esaminare ed eseguire le operazioni necessarie attività prerequisite.
- Se stai utilizzando un driver SAN ONTAP, assicurati che multipath sia abilitato su tutti i tuoi cluster Kubernetes.

Fasi

1. Spostarsi dal menu Dashboard o Clusters:
   - Da **Dashboard** in Resource Summary (Riepilogo risorse), selezionare **Add** (Aggiungi) dal pannello

Clusters (Clusters).

- Nell'area di navigazione a sinistra, selezionare **Clusters**, quindi selezionare **Add Cluster** (Aggiungi cluster) dalla pagina Clusters (Cluster).

2. Nella finestra **Add Cluster** che si apre, caricare un `kubeconfig.yaml` archiviare o incollare il contenuto di a. `kubeconfig.yaml` file.

   Il `kubeconfig.yaml` il file deve includere **solo le credenziali del cluster per un cluster**.

   Se crei il tuo `kubeconfig` file, è necessario definire solo **un** elemento di contesto al suo interno. Fare riferimento a. "Documentazione Kubernetes" per informazioni sulla creazione `kubeconfig` file. Se hai creato un kubeconfig per un ruolo cluster limitato utilizzando il processo descritto sopra, assicurarsi di caricare o incollare il kubeconfig in questa fase.

3. Fornire un nome di credenziale. Per impostazione predefinita, il nome della credenziale viene compilato automaticamente come nome del cluster.
4. Selezionare **Avanti**.
5. Selezionare la classe di storage predefinita da utilizzare per il cluster Kubernetes e selezionare **Avanti**.

   Selezionare una classe di storage Astra Trident supportata dallo storage ONTAP.

6. Esaminare le informazioni e, se tutto sembra buono, selezionare **Aggiungi**.

Risultato

Il cluster passa allo stato **Discovering** e quindi passa a **Healthy**. Ora stai gestendo il cluster con Astra Control Center.

Dopo aver aggiunto un cluster da gestire in Astra Control Center, l'implementazione dell'operatore di monitoraggio potrebbe richiedere alcuni minuti. Fino a quel momento, l'icona di notifica diventa rossa e registra un evento **Monitoring Agent Status Check Failed** (controllo stato agente non riuscito). È possibile ignorarlo, perché il problema si risolve quando Astra Control Center ottiene lo stato corretto. Se il problema non si risolve in pochi minuti, accedere al cluster ed eseguire `oc get pods -n netapp-monitoring` come punto di partenza. Per eseguire il debug del problema, consultare i log dell'operatore di monitoraggio.

Abilitare l'autenticazione sul backend dello storage ONTAP

Il centro di controllo Astra offre due modalità di autenticazione di un backend ONTAP:

- **Autenticazione basata su credenziali**: Nome utente e password di un utente ONTAP con le autorizzazioni richieste. Per garantire la massima compatibilità con le versioni di ONTAP, è necessario utilizzare un ruolo di accesso di sicurezza predefinito, ad esempio admin o vsadmin.
- **Autenticazione basata su certificato**: Il centro di controllo Astra può anche comunicare con un cluster ONTAP utilizzando un certificato installato sul back-end. Utilizzare il certificato client, la chiave e il certificato CA attendibile, se utilizzato (consigliato).

È possibile aggiornare in seguito i back-end esistenti per passare da un tipo di autenticazione a un altro metodo. È supportato un solo metodo di autenticazione alla volta.

Abilitare l'autenticazione basata su credenziali

Astra Control Center richiede le credenziali per un cluster con ambito `admin` Per comunicare con il backend ONTAP. È necessario utilizzare ruoli standard predefiniti, ad esempio `admin`. Ciò garantisce la compatibilità con le future release di ONTAP che potrebbero esporre le API delle funzionalità da utilizzare nelle future release di Astra Control Center.

> Un ruolo di accesso di sicurezza personalizzato può essere creato e utilizzato con Astra Control Center, ma non è consigliato.

Un esempio di definizione di backend è simile al seguente:

```
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "admin",
  "password": "secret"
}
```

La definizione di backend è l'unica posizione in cui le credenziali vengono memorizzate in testo normale. La creazione o l'aggiornamento di un backend è l'unico passaggio che richiede la conoscenza delle credenziali. Pertanto, si tratta di un'operazione di sola amministrazione, che deve essere eseguita da Kubernetes o dall'amministratore dello storage.

Abilitare l'autenticazione basata su certificato

Il centro di controllo Astra può utilizzare i certificati per comunicare con i backend ONTAP nuovi ed esistenti. Inserire le seguenti informazioni nella definizione di backend.

- `clientCertificate`: Certificato del client.
- `clientPrivateKey`: Chiave privata associata.
- `trustedCACertificate`: Certificato CA attendibile. Se si utilizza una CA attendibile, è necessario fornire questo parametro. Questa operazione può essere ignorata se non viene utilizzata alcuna CA attendibile.

È possibile utilizzare uno dei seguenti tipi di certificati:

- Certificato autofirmato
- Certificato di terze parti

Abilitare l'autenticazione con un certificato autofirmato

Un workflow tipico prevede i seguenti passaggi.

Fasi

1. Generare un certificato e una chiave del client. Durante la generazione, impostare il nome comune (CN) sull'utente ONTAP per l'autenticazione come.

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout k8senv.key
-out k8senv.pem -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=<common-name>"
```

2. Installare il certificato client di tipo `client-ca` E sul cluster ONTAP.

```
security certificate install -type client-ca -cert-name <certificate-
name> -vserver <vserver-name>
security ssl modify -vserver <vserver-name> -client-enabled true
```

3. Verificare che il ruolo di accesso di sicurezza di ONTAP supporti il metodo di autenticazione del certificato.

```
security login create -user-or-group-name vsadmin -application ontapi
-authentication-method cert -vserver <vserver-name>
security login create -user-or-group-name vsadmin -application http
-authentication-method cert -vserver <vserver-name>
```

4. Verificare l'autenticazione utilizzando il certificato generato. Sostituire <LIF di gestione ONTAP> e <vserver name> con l'IP LIF di gestione e il nome SVM. Assicurarsi che la politica di servizio di LIF sia impostata su `default-data-management`.

```
curl -X POST -Lk https://<ONTAP-Management-
LIF>/servlets/netapp.servlets.admin.XMLrequest_filer --key k8senv.key
--cert ~/k8senv.pem -d '<?xml version="1.0" encoding="UTF-8"?><netapp
xmlns=http://www.netapp.com/filer/admin version="1.21" vfiler="<vserver-
name>"><vserver-get></vserver-get></netapp>
```

5. Utilizzando i valori ottenuti dal passaggio precedente, aggiungere il backend di storage nell'interfaccia utente di Astra Control Center.

Abilitare l'autenticazione con un certificato di terze parti

Se si dispone di un certificato di terze parti, è possibile configurare l'autenticazione basata su certificato con questa procedura.

Fasi

1. Generare la chiave privata e la CSR:

```
openssl req -new -newkey rsa:4096 -nodes -sha256 -subj "/" -outform pem
-out ontap_cert_request.csr -keyout ontap_cert_request.key -addext
"subjectAltName = DNS:<ONTAP_CLUSTER_FQDN_NAME>,IP:<ONTAP_MGMT_IP>”
```

2. Passare la CSR alla CA di Windows (CA di terze parti) e rilasciare il certificato firmato.
3. Scarica il certificato firmato e chiamalo `ontap_signed_cert.crt'
4. Esportare il certificato root dalla CA di Windows (CA di terze parti).
5. Assegnare un nome al file `ca_root.crt`

   A questo punto, sono disponibili i seguenti tre file:

   - **Chiave privata**: `ontap_signed_request.key` (Chiave corrispondente al certificato del server in ONTAP). È necessario durante l'installazione del certificato del server).
   - **Certificato firmato**: `ontap_signed_cert.crt` (Questo è anche chiamato *certificato del server* in ONTAP).
   - **Certificato CA root**: `ca_root.crt` (Questo è anche chiamato *certificato server-ca* in ONTAP).
6. Installare questi certificati in ONTAP. Generare e installare `server` e. `server-ca` Certificati su ONTAP.

Espandere per sample.yaml

```
# Copy the contents of ca_root.crt and use it here.

security certificate install -type server-ca

Please enter Certificate: Press <Enter> when done

-----BEGIN CERTIFICATE-----
<certificate details>
-----END CERTIFICATE-----


You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:

CA:
serial:

The certificate's generated name for reference:


===

# Copy the contents of ontap_signed_cert.crt and use it here. For
key, use the contents of ontap_cert_request.key file.
security certificate install -type server
Please enter Certificate: Press <Enter> when done

-----BEGIN CERTIFICATE-----
<certificate details>
-----END CERTIFICATE-----

Please enter Private Key: Press <Enter> when done

-----BEGIN PRIVATE KEY-----
<private key details>
-----END PRIVATE KEY-----

Enter certificates of certification authorities (CA) which form the
certificate chain of the server certificate. This starts with the
issuing CA certificate of the server certificate and can range up to
the root CA certificate.
Do you want to continue entering root and/or intermediate
```

```
certificates {y|n}: n

The provided certificate does not have a common name in the subject
field.
Enter a valid common name to continue installation of the
certificate: <ONTAP_CLUSTER_FQDN_NAME>

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.
The installed certificate's CA and serial number for reference:
CA:
serial:
The certificate's generated name for reference:


==
# Modify the vserver settings to enable SSL for the installed
certificate

ssl modify -vserver <vserver_name> -ca <CA>  -server-enabled true
-serial <serial number>       (security ssl modify)

==
# Verify if the certificate works fine:

openssl s_client -CAfile ca_root.crt -showcerts -servername server
-connect <ONTAP_CLUSTER_FQDN_NAME>:443
CONNECTED(00000005)
depth=1 DC = local, DC = umca, CN = <CA>
verify return:1
depth=0
verify return:1
write W BLOCK
---
Certificate chain
0 s:
   i:/DC=local/DC=umca/<CA>

-----BEGIN CERTIFICATE-----
<Certificate details>
```

7. Creare il certificato client per lo stesso host per le comunicazioni senza password. Il centro di controllo Astra utilizza questo processo per comunicare con ONTAP.
8. Generare e installare i certificati client su ONTAP:

Espandere per sample.yaml

```
# Use /CN=admin or use some other account which has privileges.
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout
ontap_test_client.key -out ontap_test_client.pem -subj "/CN=admin"

Copy the content of ontap_test_client.pem file and use it in the
below command:
security certificate install -type client-ca -vserver <vserver_name>

Please enter Certificate: Press <Enter> when done

-----BEGIN CERTIFICATE-----
<Certificate details>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.
The installed certificate's CA and serial number for reference:

CA:
serial:
The certificate's generated name for reference:


==

ssl modify -vserver <vserver_name> -client-enabled true
(security ssl modify)

# Setting permissions for certificates
security login create -user-or-group-name admin -application ontapi
-authentication-method cert -role admin -vserver <vserver_name>

security login create -user-or-group-name admin -application http
-authentication-method cert -role admin -vserver <vserver_name>

==

#Verify passwordless communication works fine with the use of only
certificates:

curl --cacert ontap_signed_cert.crt  --key ontap_test_client.key
--cert ontap_test_client.pem
https://<ONTAP_CLUSTER_FQDN_NAME>/api/storage/aggregates
{
```

```
"records": [
{
"uuid": "f84e0a9b-e72f-4431-88c4-4bf5378b41bd",
"name": "<aggr_name>",
"node": {
"uuid": "7835876c-3484-11ed-97bb-d039ea50375c",
"name": "<node_name>",
"_links": {
"self": {
"href": "/api/cluster/nodes/7835876c-3484-11ed-97bb-d039ea50375c"
}
}
},
"_links": {
"self": {
"href": "/api/storage/aggregates/f84e0a9b-e72f-4431-88c4-
4bf5378b41bd"
}
}
}
],
"num_records": 1,
"_links": {
"self": {
"href": "/api/storage/aggregates"
}
}
}%
```


9. Aggiungere il backend dello storage nell'interfaccia utente di Astra Control Center e fornire i seguenti valori:
   - **Certificato client**: ontap_test_client.pem
   - **Chiave privata**: ontap_test_client.key
   - **Certificato CA attendibile**: ontap_signed_cert.crt

Aggiungere un backend di storage

Dopo aver impostato le credenziali o le informazioni di autenticazione del certificato, è possibile aggiungere un backend di storage ONTAP esistente a Astra Control Center per gestire le risorse.

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.

Astra Control Provisioner only: L'aggiunta e la gestione di backend di storage ONTAP in Astra Control Center è opzionale quando si utilizza la tecnologia NetApp SnapMirror se si è attivato Astra Control Provisioner con Astra Control Center 23,10 o versioni successive.

Fasi

1. Dal pannello di controllo nell'area di navigazione a sinistra, selezionare **Backend**.
2. Selezionare **Aggiungi**.
3. Nella sezione Use existing della pagina Add storage backend, selezionare **ONTAP**.
4. Selezionare una delle seguenti opzioni:
   - **Usa credenziali amministratore**: Inserire l'indirizzo IP di gestione del cluster ONTAP e le credenziali di amministratore. Le credenziali devono essere credenziali a livello di cluster.

     L'utente di cui si inseriscono le credenziali deve disporre di `ontapi` Metodo di accesso all'accesso dell'utente abilitato in Gestione di sistema di ONTAP sul cluster ONTAP. Se si intende utilizzare la replica SnapMirror, applicare le credenziali utente con il ruolo "admin", che dispone dei metodi di accesso `ontapi` e. `http`, Sui cluster ONTAP di origine e di destinazione. Fare riferimento a. "Gestire gli account utente nella documentazione di ONTAP" per ulteriori informazioni.

   - **Usa un certificato**: Carica il certificato `.pem` file, la chiave del certificato `.key` e, facoltativamente, il file dell'autorità di certificazione.
5. Selezionare **Avanti**.
6. Confermare i dettagli del back-end e selezionare **Manage** (Gestisci).

Risultato

Il backend viene visualizzato in `online` indicare nell'elenco le informazioni di riepilogo.

Potrebbe essere necessario aggiornare la pagina per visualizzare il backend.

Aggiungi un bucket

È possibile aggiungere un bucket utilizzando l'interfaccia utente di Astra Control o. "API di controllo Astra". L'aggiunta di provider di bucket di archivi 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. Astra Control memorizza i backup o i cloni nei bucket dell'archivio di oggetti definiti dall'utente.

Non è necessario un bucket in Astra Control se si esegue il cloning della configurazione dell'applicazione e dello storage persistente sullo stesso cluster. La funzionalità di snapshot delle applicazioni non richiede un bucket.

Prima di iniziare

- Assicurati di avere un bucket raggiungibile dai cluster gestiti da Astra Control Center.
- Assicurarsi di disporre delle credenziali per il bucket.
- Assicurarsi che la benna sia di uno dei seguenti tipi:
  - NetApp ONTAP S3
  - NetApp StorageGRID S3
  - Microsoft Azure
  - Generico S3

Amazon Web Services (AWS) e Google Cloud Platform (GCP) utilizzano il tipo di bucket S3 generico.

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 rivendicano il supporto S3 di Amazon.

Fasi

1. Nell'area di navigazione a sinistra, selezionare **Bucket**.
2. Selezionare **Aggiungi**.
3. Selezionare il tipo di bucket.

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

4. Inserire un nome bucket esistente e una descrizione opzionale.

   Il nome e la descrizione del bucket vengono visualizzati come una posizione di backup che è possibile scegliere in seguito quando si crea un backup. Il nome viene visualizzato anche durante la configurazione del criterio di protezione.

5. Inserire il nome o l'indirizzo IP dell'endpoint S3.
6. In **Seleziona credenziali**, selezionare la scheda **Aggiungi** o **Usa esistente**.
   - Se si sceglie **Aggiungi**:
     i. Immettere un nome per la credenziale che la distingue dalle altre credenziali in Astra Control.
     ii. Inserire l'ID di accesso e la chiave segreta incollando il contenuto dagli Appunti.
   - Se si sceglie **Usa esistente**:
     i. Selezionare le credenziali esistenti che si desidera utilizzare con il bucket.
7. Selezionare `Add`.

   Quando si aggiunge un bucket, Astra Control contrassegna un bucket con l'indicatore bucket predefinito. Il primo bucket creato diventa quello predefinito. Con l'aggiunta di bucket, è possibile decidere in un secondo momento "impostare un altro bucket predefinito".

Quali sono le prossime novità?

Ora che hai effettuato l'accesso e aggiunto i cluster ad Astra Control Center, sei pronto per iniziare a utilizzare le funzionalità di gestione dei dati delle applicazioni di Astra Control Center.

- "Gestire utenti e ruoli locali"
- "Inizia a gestire le app"
- "Proteggi le app"
- "Gestire le notifiche"

- "Connettersi a Cloud Insights"
- "Aggiungere un certificato TLS personalizzato"
- "Modificare la classe di storage predefinita"

Trova ulteriori informazioni

- "Utilizzare l'API di controllo Astra"
- "Problemi noti"

Domande frequenti per Astra Control Center

Queste FAQ possono essere utili se stai cercando una risposta rapida a una domanda.

Panoramica

Le sezioni seguenti forniscono risposte ad alcune domande aggiuntive che potrebbero essere presentate durante l'utilizzo di Astra Control Center. Per ulteriori chiarimenti, contatta il sito astra.feedback@netapp.com

Accesso al centro di controllo Astra

Cos'è l'URL di Astra Control?

Astra Control Center utilizza l'autenticazione locale e un URL specifico per ciascun ambiente.

Per l'URL, in un browser, immettere il nome di dominio completo (FQDN) impostato nel campo spec.astraAddress nel file di risorsa personalizzata (CR) astra_control_center.yaml quando si installa Astra Control Center. L'email è il valore impostato nel campo spec.email in astra_control_center.yaml CR.

Licensing

Utilizzo una licenza di valutazione. Come si passa alla licenza completa?

È possibile passare facilmente a una licenza completa ottenendo il file di licenza NetApp (NLF) da NetApp.

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **account** > **licenza**.
2. Nella panoramica della licenza, a destra delle informazioni sulla licenza, selezionare il menu Opzioni.
3. Selezionare **Sostituisci**.
4. Individuare il file di licenza scaricato e selezionare **Aggiungi**.

Utilizzo una licenza di valutazione. Posso comunque gestire le applicazioni?

Sì, è possibile testare la funzionalità di gestione delle applicazioni con una licenza di valutazione (inclusa la licenza di valutazione integrata installata per impostazione predefinita). Non vi è alcuna differenza in termini di funzionalità tra una licenza di valutazione e una licenza completa; la licenza di valutazione ha semplicemente una durata inferiore. Fare riferimento a. "Licensing" per ulteriori informazioni.

Registrazione dei cluster Kubernetes

Devo aggiungere nodi di lavoro al cluster Kubernetes dopo l'aggiunta ad Astra Control. Cosa devo fare?

È possibile aggiungere nuovi nodi di lavoro ai pool esistenti. Questi verranno rilevati automaticamente da Astra Control. Se i nuovi nodi non sono visibili in Astra Control, controllare se i nuovi nodi di lavoro eseguono il tipo di immagine supportato. È inoltre possibile verificare lo stato dei nuovi nodi di lavoro utilizzando `kubectl get nodes` comando.

Come si annulla la gestione corretta di un cluster?

1. "Annulla la gestione delle applicazioni da Astra Control".
2. "Annullare la gestione del cluster da Astra Control".

Cosa succede alle mie applicazioni e ai miei dati dopo aver rimosso il cluster Kubernetes da Astra Control?

La rimozione di un cluster da Astra Control non apporta alcuna modifica alla configurazione del cluster (applicazioni e storage persistente). Eventuali snapshot di Astra Control o backup delle applicazioni su quel cluster non saranno disponibili per il ripristino. I backup persistenti dello storage creati da Astra Control rimangono all'interno di Astra Control, ma non sono disponibili per il ripristino.

> Rimuovere sempre un cluster da Astra Control prima di eliminarlo con altri metodi. L'eliminazione di un cluster utilizzando un altro tool mentre viene ancora gestito da Astra Control può causare problemi all'account Astra Control.

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

Gestione delle applicazioni

Astra Control può implementare un'applicazione?

Astra Control non implementa le applicazioni. Le applicazioni devono essere implementate all'esterno di Astra Control.

Cosa succede alle applicazioni dopo che non li gestisco da Astra Control?

Eventuali backup o snapshot esistenti verranno eliminati. Le applicazioni e i dati rimangono disponibili. Le operazioni di gestione dei dati non saranno disponibili per le applicazioni non gestite o per eventuali backup o snapshot ad esse appartenenti.

- Astra Control può gestire un'applicazione su storage non NetApp?*

No Anche se Astra Control è in grado di rilevare applicazioni che utilizzano storage non NetApp, non è in grado di gestire un'applicazione che utilizza storage non NetApp.

Dovrei gestire Astra Control da solo?

Astra Control Center non viene mostrato per impostazione predefinita come un'applicazione che puoi gestire, ma puoi farlo "eseguire il backup e il ripristino" Un'istanza di Astra Control Center che utilizza un'altra istanza di

Astra Control Center.

I pod malsani influiscono sulla gestione delle applicazioni?

No, la salute dei pod non influisce sulla gestione delle app.

Operazioni di gestione dei dati

La mia applicazione utilizza diversi PVS. Astra Control eseguirà snapshot e backup di questi PVS?

Sì. Un'operazione snapshot su un'applicazione di Astra Control include snapshot di tutti i PVS associati ai PVC dell'applicazione.

È possibile gestire le snapshot acquisite da Astra Control direttamente attraverso un'interfaccia o un'archiviazione a oggetti diversa?

No Snapshot e backup creati da Astra Control possono essere gestiti solo con Astra Control.

Astra Control provisioner

In che modo le funzionalità di provisioning dello storage di Astra Control Provivisioner sono diverse da quelle di Astra Trident?

Astra Control Provivisioner, in qualità di parte di Astra Control, supporta un superset di funzionalità di provisioning dello storage che non sono disponibili in Astra Trident, open-source. Queste funzionalità si aggiungono a tutte le funzionalità disponibili per Trident open-source.

Astra Control Provisioner sostituisce Astra Trident?

In arrivo gli update di Astra Control, Astra Control Provivisioner sostituirà Astra Trident come provisioner di storage e orchestrator nell'architettura Astra Control. Pertanto, è vivamente consigliato agli utenti di Astra Control "Abilita Astra Control Provisioner". Astra Trident continuerà a rimanere open source e ad essere rilasciato, mantenuto, supportato e aggiornato con le nuove CSI e altre funzionalità di NetApp.

Devo pagare per Astra Trident?

No Astra Trident continuerà a essere open source e scaricabile gratuitamente.

È possibile utilizzare le funzionalità di gestione e provisioning dello storage di Astra Control senza installare e utilizzare Astra Control?

Sì, puoi eseguire l'aggiornamento a Astra Trident 23,10 o versione successiva e attivare la funzionalità Astra Control Provivisioner anche se non vuoi utilizzare il set completo di funzionalità di gestione dei dati di Astra Control.

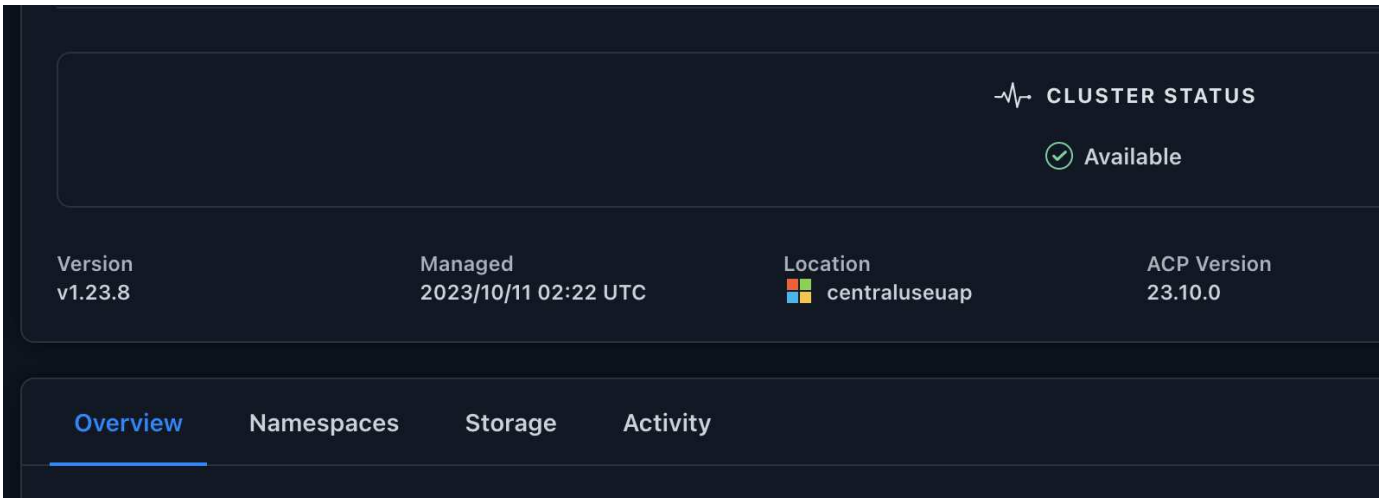
Come posso passare da un utente Trident esistente a Astra Control per utilizzare funzionalità avanzate di provisioning e gestione dello storage?

Se sei un utente Trident (compresi gli utenti di Astra Trident nel cloud pubblico), devi prima acquistare una licenza Astra Control. Dopo che avrai fatto, puoi scaricare il bundle Astra Control Provivisioner, eseguire l'upgrade di Astra Trident e. "Attiva la funzionalità Astra Control Provisioner".

Come faccio a sapere se Astra Control Provivisioner ha sostituito Astra Trident sul mio cluster?

Dopo l'installazione di Astra Control Provisioner, il cluster host nell'interfaccia utente di Astra Control mostrerà

un `ACP version` piuttosto che `Trident version` campo e numero della versione installata corrente.



Se non si dispone dell'accesso all'interfaccia utente, è possibile confermare la corretta installazione utilizzando i seguenti metodi:

Operatore Astra Trident

Verificare `trident-acp` il container è in esecuzione e così `acpVersion` è `23.10.0` con stato di `Installed`:

```
kubectl get torc -o yaml
```

Risposta:

```
status:
  acpVersion: 23.10.0
  currentInstallationParams:
    ...
    acpImage: <my_custom_registry>/trident-acp:23.10.0
    enableACP: "true"
    ...
  ...
  status: Installed
```

tridentctl

Confermare che Astra Control Provisioner è stato abilitato:

```
./tridentctl -n trident version
```

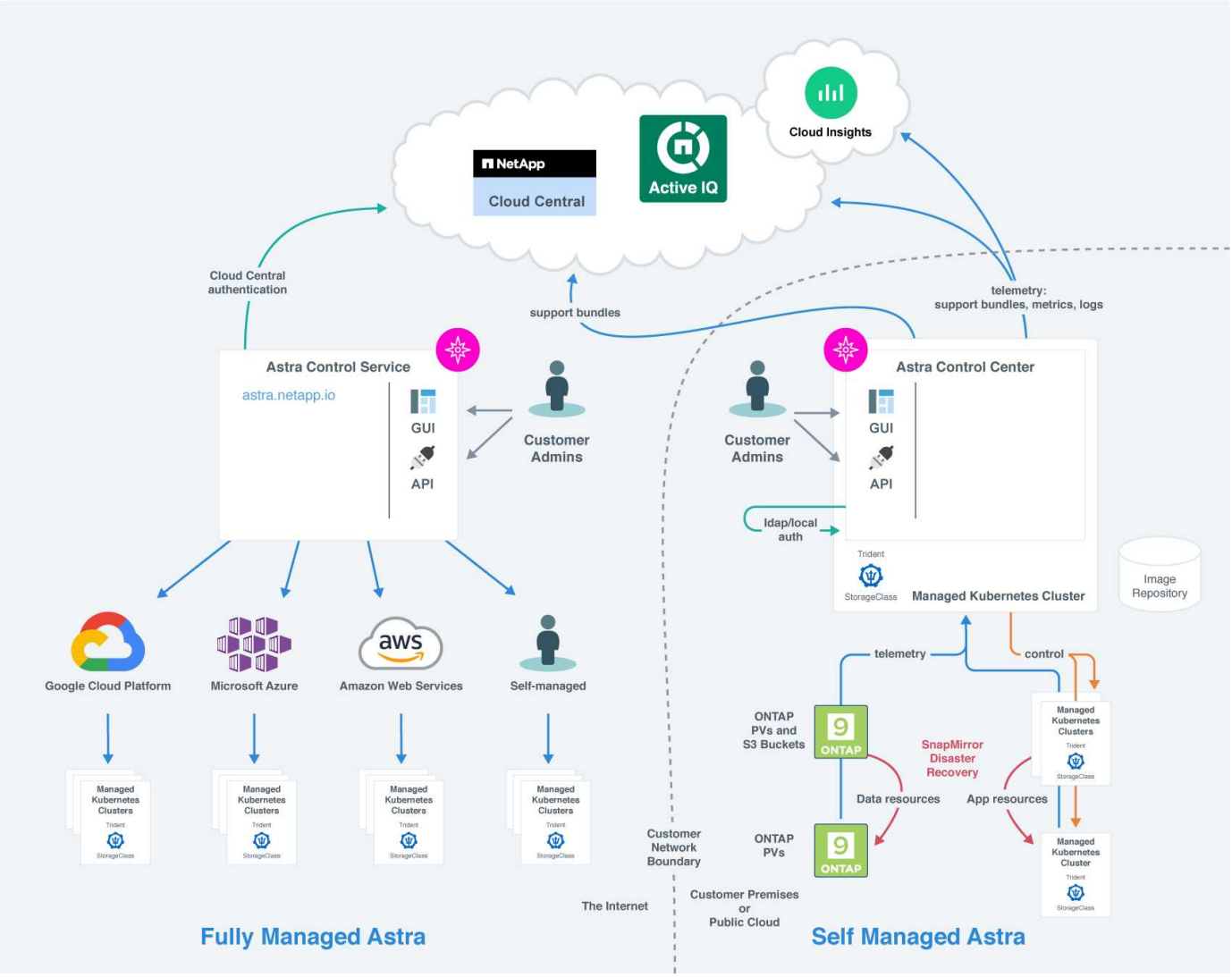
Risposta:

```
+----------------+----------------+-------------+ | SERVER VERSION |
CLIENT VERSION | ACP VERSION | +----------------+----------------
+-------------+ | 23.10.0 | 23.10.0 | 23.10.0. | +----------------
+----------------+-------------+
```

Concetti

Architettura e componenti

Ecco una panoramica dei vari componenti dell'ambiente Astra Control.



Componenti di controllo Astra

- **Kubernetes Clusters**: Kubernetes è una piattaforma open-source portatile, estensibile per la gestione di carichi di lavoro e servizi containerizzati, che facilita sia la configurazione dichiarativa che l'automazione. Astra fornisce servizi di gestione per le applicazioni ospitate in un cluster Kubernetes.
- * Astra Trident*: In qualità di provider di storage open source e orchestrator gestiti da NetApp, Astra Trident consente di creare volumi di storage per applicazioni containerizzate gestite da Docker e Kubernetes. Se implementato con il centro di controllo Astra, Astra Trident include un backend di storage ONTAP configurato.
- **Storage backend**:
  - Astra Control Service utilizza i seguenti backend di storage:
    - "NetApp Cloud Volumes Service per Google Cloud" O Google Persistent Disk come backend di

storage per i cluster GKE

        - "Azure NetApp Files" O Azure Managed Disks come backend di storage per i cluster AKS.
        - "Amazon Elastic Block Store (EBS)" oppure "Amazon FSX per NetApp ONTAP" Come opzioni di storage back-end per i cluster EKS.
    - Astra Control Center utilizza i seguenti backend di storage:
        - ONTAP AFF, FAS e ASA. In qualità di piattaforma hardware e software per lo storage, ONTAP offre servizi di storage di base, supporto per più protocolli di accesso allo storage e funzionalità di gestione dello storage, come snapshot e mirroring.
        - Cloud Volumes ONTAP
- **Cloud Insights**: Uno strumento di monitoraggio dell'infrastruttura cloud di NetApp, Cloud Insights consente di monitorare le performance e l'utilizzo dei cluster Kubernetes gestiti dal centro di controllo Astra. Cloud Insights mette in relazione l'utilizzo dello storage con i carichi di lavoro. Quando si attiva la connessione Cloud Insights in Astra Control Center, le informazioni di telemetria vengono visualizzate nelle pagine dell'interfaccia utente di Astra Control Center.

Interfacce di controllo Astra

È possibile completare le attività utilizzando diverse interfacce:

- **Interfaccia utente Web (UI)**: Sia Astra Control Service che Astra Control Center utilizzano la stessa interfaccia utente basata sul Web, in cui è possibile gestire, migrare e proteggere le applicazioni. Utilizzare l'interfaccia utente anche per gestire gli account utente e le impostazioni di configurazione.
- **API**: Sia Astra Control Service che Astra Control Center utilizzano la stessa API Astra Control. Utilizzando l'API, è possibile eseguire le stesse attività dell'interfaccia utente.

Astra Control Center consente inoltre di gestire, migrare e proteggere i cluster Kubernetes in esecuzione negli ambienti delle macchine virtuali.

Per ulteriori informazioni

- "Documentazione del servizio Astra Control"
- "Documentazione di Astra Control Center"
- "Documentazione di Astra Trident"
- "Utilizzare l'API di controllo Astra"
- "Documentazione Cloud Insights"
- "Documentazione ONTAP"

Protezione dei dati

Scopri i tipi di protezione dei dati disponibili in Astra Control Center e come utilizzarli al meglio per proteggere le tue applicazioni.

Snapshot, backup e policy di protezione

Sia le snapshot che i backup proteggono i seguenti tipi di dati:

- L'applicazione stessa

- Tutti i volumi di dati persistenti associati all'applicazione
- Qualsiasi elemento di risorsa appartenente all'applicazione

Una *snapshot* è una copia point-in-time di un'applicazione memorizzata sullo stesso volume fornito dell'applicazione. Di solito sono veloci. È possibile utilizzare snapshot locali 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. Le snapshot sono utili per clonare o ripristinare un'applicazione all'interno dello stesso cluster.

Un *backup* si basa su uno snapshot. Viene memorizzato nell'archivio di oggetti esterno e, per questo motivo, può essere più lento rispetto agli snapshot locali. È possibile ripristinare un backup dell'applicazione nello stesso cluster oppure migrare un'applicazione ripristinando il backup su un cluster diverso. È inoltre possibile scegliere un periodo di conservazione più lungo per i backup. Poiché sono memorizzati nell'archivio di oggetti esterno, i backup offrono in genere una protezione migliore rispetto alle snapshot in caso di guasto al server o perdita di dati.

Una *policy di protezione* è un metodo per proteggere un'applicazione creando automaticamente snapshot, backup o entrambi in base a un programma definito per tale applicazione. Una policy di protezione consente inoltre di scegliere il numero di snapshot e backup da conservare nella pianificazione e di impostare diversi livelli di granularità della pianificazione. L'automazione di backup e snapshot con una policy di protezione è il modo migliore per garantire che ogni applicazione sia protetta in base alle esigenze della tua organizzazione e ai requisiti SLA (Service Level Agreement).

> *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 associato, è necessario un backup per il ripristino. Un'istantanea non consentirebbe il ripristino.

Backup immutabili

Un backup immutabile è un backup che non può essere modificato o eliminato durante un periodo specificato. Quando crei un backup immutabile, Astra Control controlla che il bucket che stai utilizzando sia un bucket WORM (Write Once Read Many) e, in caso affermativo, garantisce che il backup sia immutabile dall'interno di Astra Control.
Astra Control Center supporta la creazione di backup immutabili con le seguenti piattaforme e tipi di bucket:

- Amazon Web Services che utilizza un bucket Amazon S3 con blocco oggetti S3 configurato
- NetApp StorageGRID che utilizza un bucket S3 con blocco oggetto S3 configurato

Tenere presente quanto segue quando si utilizzano i backup immutabili:

- Se si esegue il backup in un bucket WORM in una piattaforma non supportata o in un tipo di bucket non supportato, si potrebbero ottenere risultati imprevedibili, come il mancato completamento dell'eliminazione del backup anche se è trascorso il tempo di conservazione.
- Astra Control non supporta le policy di data Lifecycle management o l'eliminazione manuale di oggetti nei bucket utilizzati con backup immutabili. Verifica che il back-end dello storage non sia configurato per gestire il ciclo di vita delle snapshot di Astra Control o dei dati di cui è stato eseguito il backup.

Cloni

Un *clone* è un duplicato esatto di un'applicazione, della sua configurazione e dei suoi volumi di dati persistenti. È possibile creare manualmente un clone sullo stesso cluster Kubernetes o su un altro cluster. La clonazione di un'applicazione può essere utile se è necessario spostare applicazioni e storage da un cluster Kubernetes a

un altro.

Replica tra back-end dello storage

Grazie ad Astra Control, puoi creare business continuity per le tue applicazioni con un RPO (Recovery Point Objective) basso e un RTO basso (Recovery Time Objective) utilizzando le funzionalità di replica asincrona della tecnologia NetApp SnapMirror. Una volta configurata, questa opzione consente alle applicazioni di replicare le modifiche dei dati e delle applicazioni da un backend di storage all'altro, sullo stesso cluster o tra cluster diversi.

È possibile eseguire la replica tra due SVM ONTAP sullo stesso cluster ONTAP o su diversi cluster ONTAP.

Astra Control replica in modo asincrono le copie snapshot delle applicazioni in un cluster di destinazione. Il processo di replica include i dati nei volumi persistenti replicati da SnapMirror e i metadati dell'applicazione protetti da Astra Control.

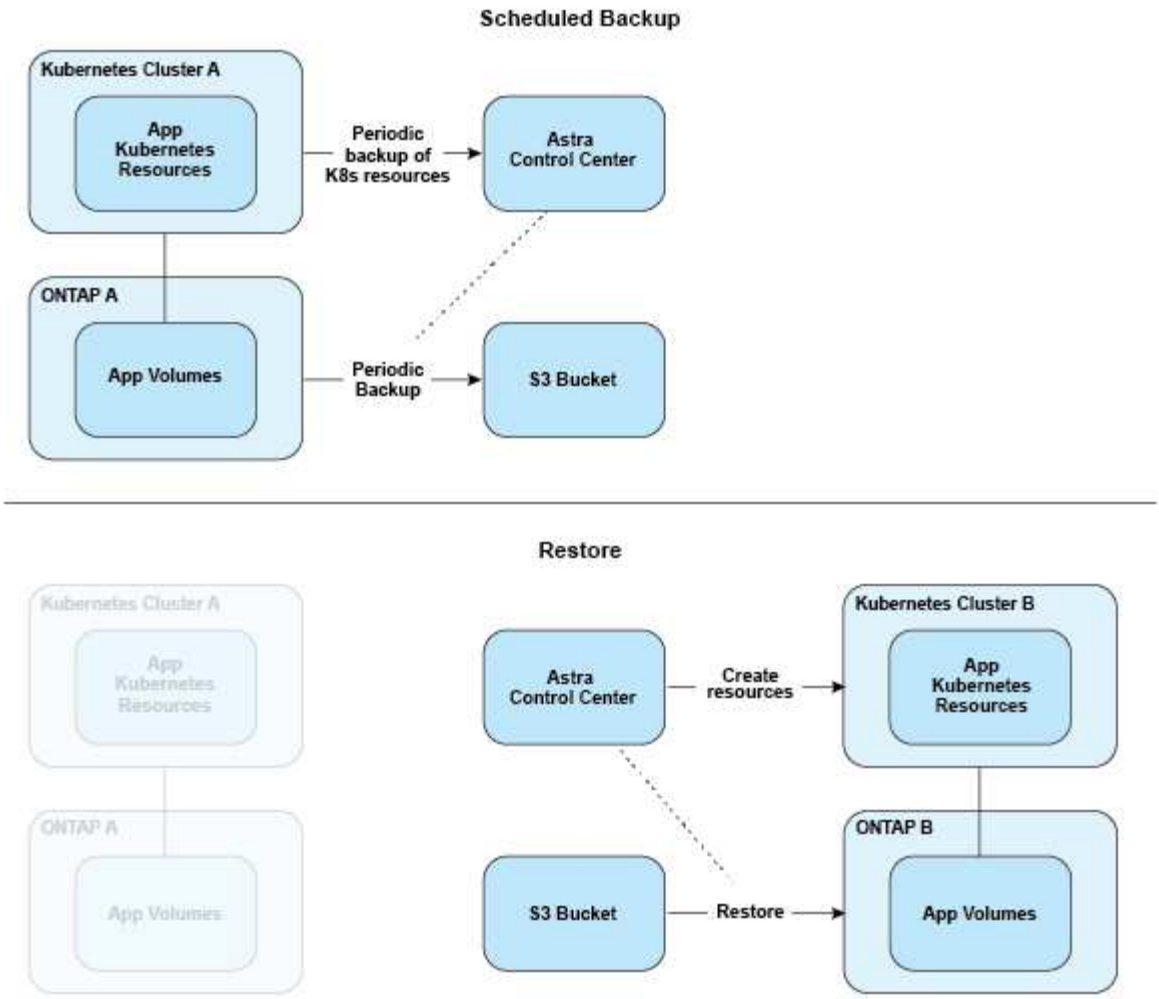
La replica dell'app è diversa dal backup e ripristino dell'app nei seguenti modi:

- **Replica dell'applicazione**: Astra Control richiede che i cluster Kubernetes di origine e di destinazione (che possono essere lo stesso cluster) siano disponibili e gestiti con i rispettivi backend di storage ONTAP configurati per abilitare SnapMirror di NetApp. Astra Control prende lo snapshot applicativo basato su policy e lo replica nel back-end dello storage di destinazione. La tecnologia SnapMirror di NetApp viene utilizzata per replicare i dati dei volumi persistenti. Per eseguire il failover, Astra Control può portare online l'applicazione replicata ricreando gli oggetti dell'applicazione sul cluster Kubernetes di destinazione con i volumi replicati sul cluster ONTAP di destinazione. Poiché i dati del volume persistente sono già presenti nel cluster ONTAP di destinazione, Astra Control può offrire tempi di ripristino rapidi per il failover.
- **Backup e ripristino dell'applicazione**: Durante il backup delle applicazioni, Astra Control crea un'istantanea dei dati dell'applicazione e li memorizza in un bucket di storage a oggetti. Quando è necessario un ripristino, i dati nel bucket devono essere copiati in un volume persistente sul cluster ONTAP. L'operazione di backup/ripristino non richiede la disponibilità e la gestione del cluster Kubernetes/ONTAP secondario, ma la copia dei dati aggiuntiva può comportare tempi di ripristino più lunghi.

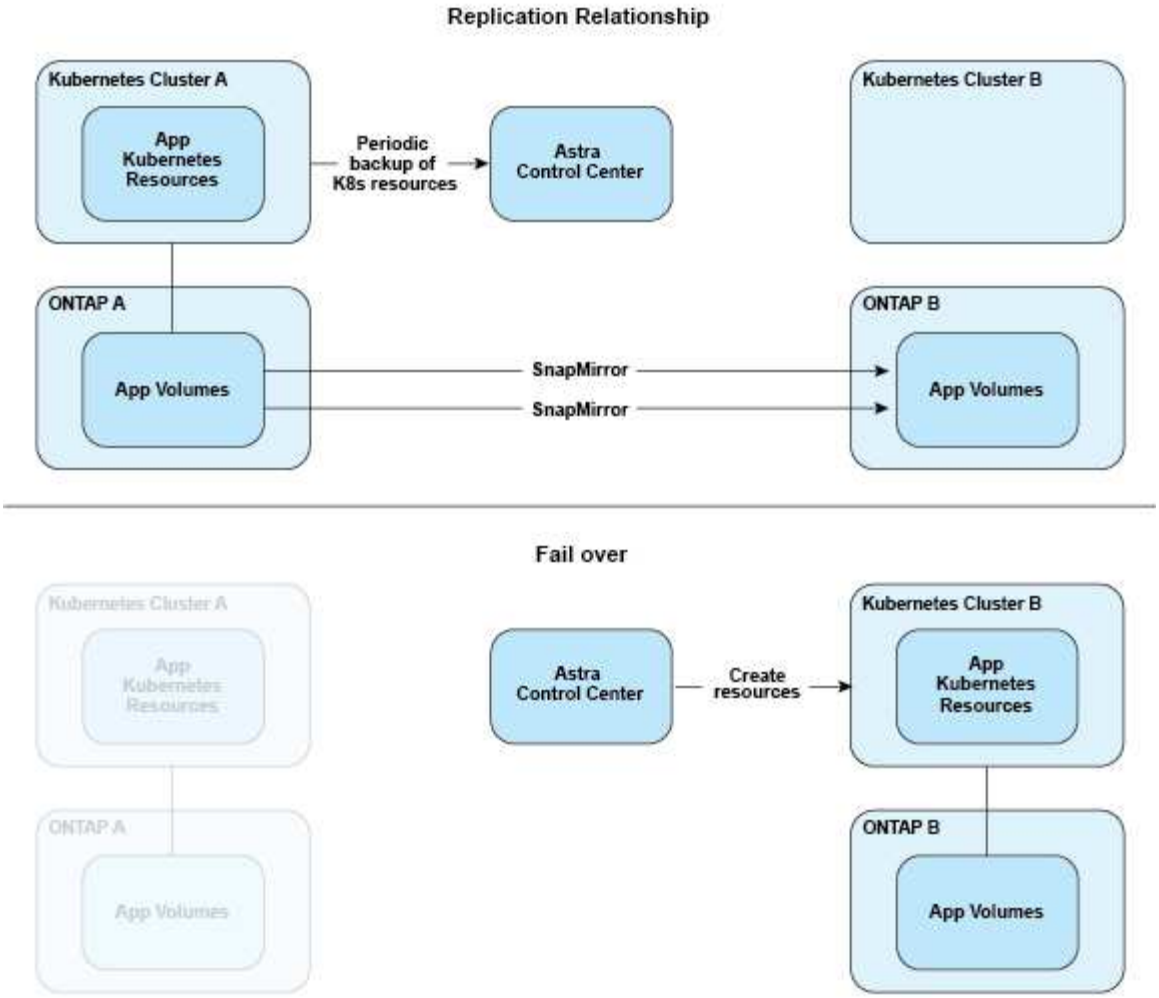
Per informazioni su come replicare le applicazioni, fare riferimento a. "Replica delle applicazioni su un sistema remoto utilizzando la tecnologia SnapMirror".

Le seguenti immagini mostrano il processo di backup e ripristino pianificato rispetto al processo di replica.

Il processo di backup copia i dati nei bucket S3 e li ripristina dai bucket S3:



D’altro canto, la replica viene eseguita replicando in ONTAP e quindi un failover crea le risorse Kubernetes:



Backup, snapshot e cloni con una licenza scaduta

Se la licenza scade, è possibile aggiungere una nuova applicazione o eseguire operazioni di protezione dell'applicazione (come snapshot, backup, cloni e operazioni di ripristino) solo se l'applicazione che si sta aggiungendo o proteggendo è un'altra istanza di Astra Control Center.

Licensing

Quando si implementa Astra Control Center, viene installato con una licenza di valutazione integrata di 90 giorni per 4,800 unità CPU. Se hai bisogno di maggiore capacità o di un periodo di valutazione più lungo, o se desideri passare a una licenza completa, puoi ottenere una licenza di valutazione o una licenza completa diversa da NetApp.

Si ottiene una licenza in uno dei seguenti modi:

- Se stai valutando Astra Control Center e hai bisogno di termini di valutazione diversi da quelli inclusi nella licenza di valutazione integrata, contatta NetApp per richiedere un file di licenza di valutazione diverso.
- "Se hai già acquistato Astra Control Center, genera il file di licenza NetApp (NLF)" Accedendo al NetApp Support Site e accedendo alle licenze software nel menu Systems.

Per ulteriori informazioni sulle licenze necessarie per i backend di storage ONTAP, fare riferimento a. "backend di storage supportati".

> Assicurarsi che la licenza consenta di utilizzare almeno tutte le unità CPU necessarie. Se il numero di unità CPU attualmente gestite da Astra Control Center supera le unità CPU disponibili nella nuova licenza applicata, non sarà possibile applicare la nuova licenza.

Licenze di valutazione e licenze complete

Una licenza di valutazione integrata viene fornita con una nuova installazione di Astra Control Center. Una licenza di valutazione offre le stesse funzionalità e funzionalità di una licenza completa per un periodo limitato (90 giorni). Dopo il periodo di valutazione, è necessaria una licenza completa per continuare con le funzionalità complete.

Scadenza della licenza

Se la licenza di Astra Control Center attiva scade, le funzionalità UI e API per le seguenti funzioni non sono disponibili:

- Snapshot e backup locali manuali
- Snapshot e backup locali pianificati
- Ripristino da uno snapshot o da un backup
- Clonazione da uno snapshot o da uno stato corrente
- Gestione di nuove applicazioni
- Configurazione dei criteri di replica

Come viene calcolato il consumo delle licenze

Quando si aggiunge un nuovo cluster ad Astra Control Center, non viene contato per ottenere licenze consumate fino a quando almeno un'applicazione in esecuzione sul cluster non viene gestita da Astra Control Center.

Quando si inizia a gestire un'applicazione su un cluster, tutte le unità CPU del cluster sono incluse nel consumo di licenza di Astra Control Center, ad eccezione delle unità CPU del nodo del cluster Red Hat OpenShift segnalate da un utilizzando l'etichetta `node-role.kubernetes.io/infra: ""`.

> I nodi dell'infrastruttura Red Hat OpenShift non consumano licenze in Astra Control Center. Per contrassegnare un nodo come nodo dell'infrastruttura, applicare l'etichetta `node-role.kubernetes.io/infra: ""` al nodo.

Trova ulteriori informazioni

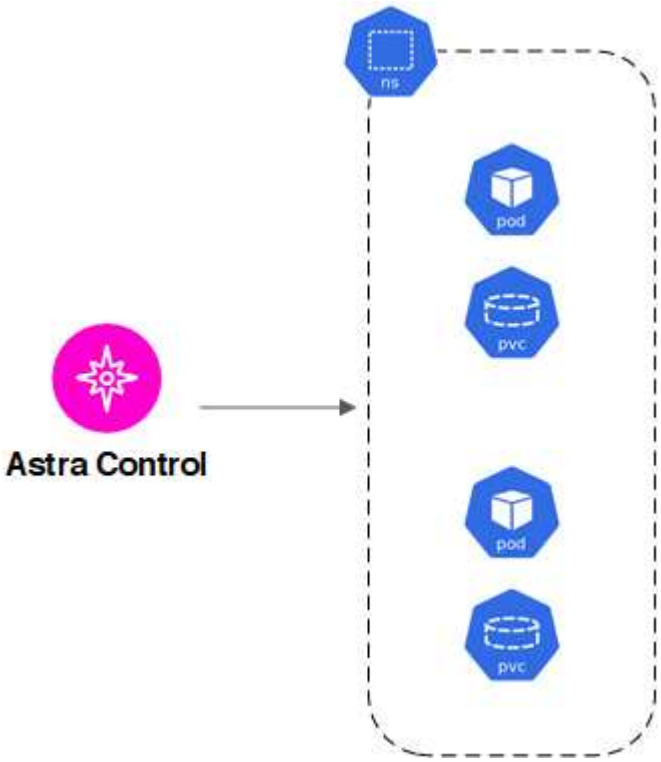
- "Aggiungere una licenza quando si imposta Astra Control Center per la prima volta"
- "Aggiornare una licenza esistente"

Gestione delle applicazioni

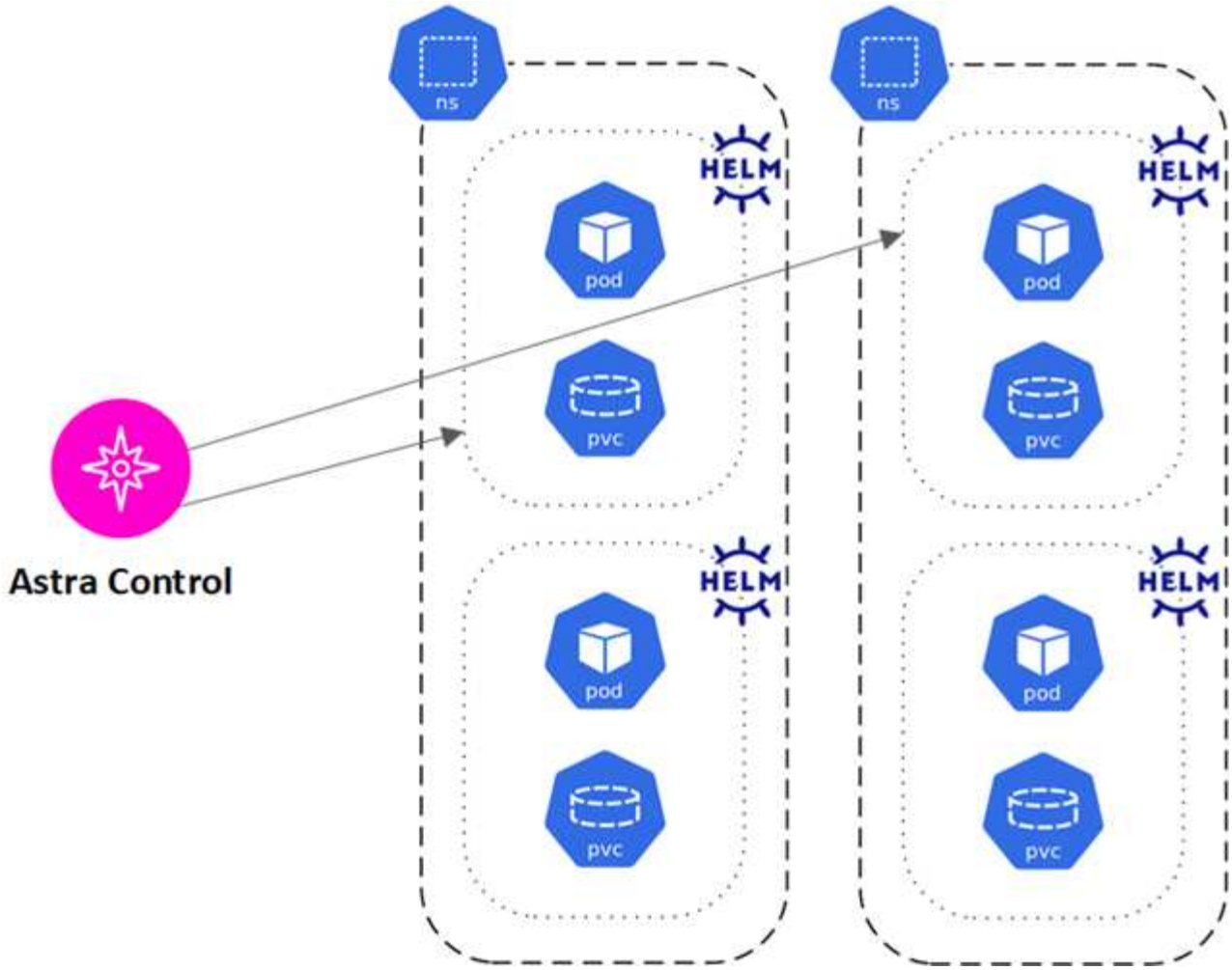
Quando Astra Control rileva i tuoi cluster, le applicazioni di questi ultimi non vengono gestite fino a quando non scegli come gestirli. Un'applicazione gestita in Astra Control

può essere una delle seguenti:

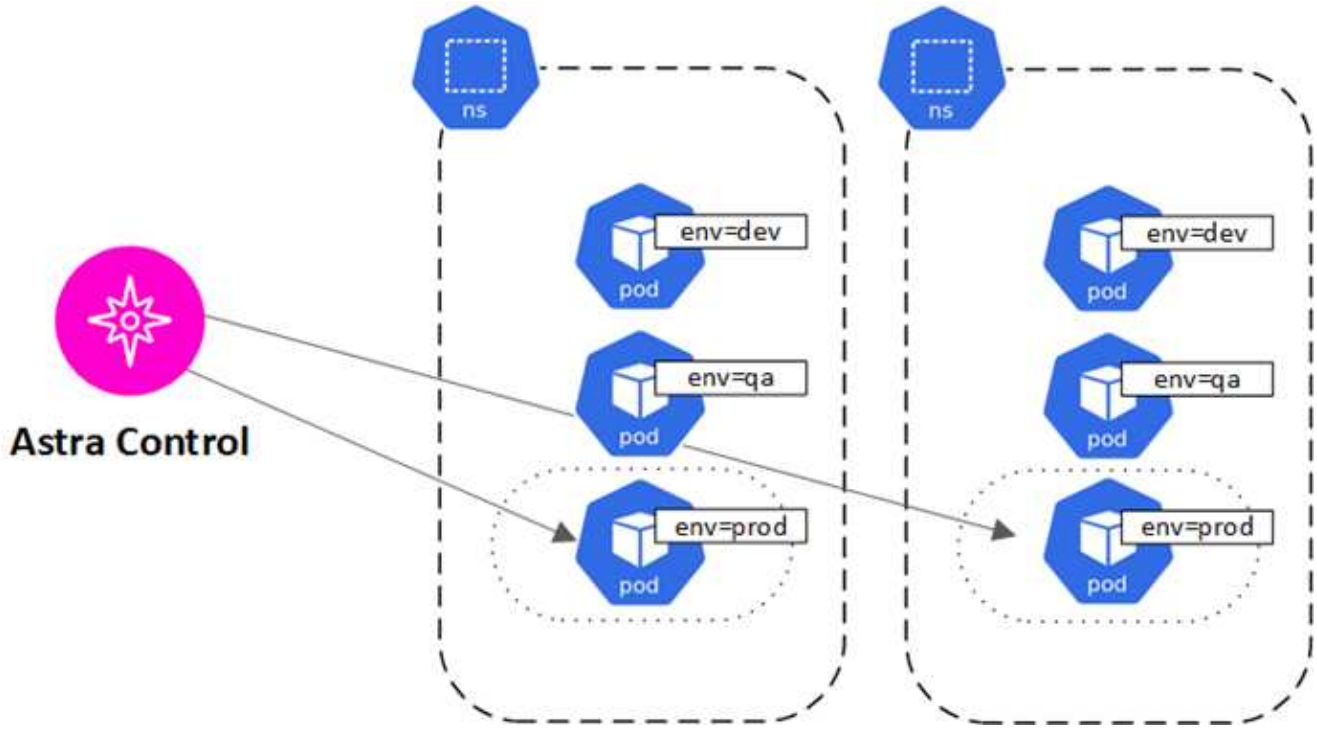
- Uno spazio dei nomi, che include tutte le risorse dello spazio dei nomi



- Una singola applicazione implementata all'interno di uno o più spazi dei nomi (in questo esempio viene utilizzato helm3)



- Un gruppo di risorse identificate da un'etichetta Kubernetes all'interno di uno o più spazi dei nomi



Classi di storage e dimensioni del volume persistente

Il centro di controllo Astra supporta NetApp ONTAP e Longhorn come backend di storage.

Panoramica

Astra Control Center supporta:

- **Astra Trident storage classes backend supportato dallo storage ONTAP**: Se si utilizza un backend ONTAP, Astra Control Center offre la possibilità di importare il backend ONTAP per la segnalazione di varie informazioni di monitoraggio.
- **Classi di storage basate su CSI supportate da Longhorn**: È possibile utilizzare Longhorn con il driver CSI (Container Storage Interface) di Longhorn.

> Le classi di storage Astra Trident devono essere preconfigurate all'esterno di Astra Control Center.

Classi di storage

Quando si aggiunge un cluster ad Astra Control Center, viene richiesto di selezionare una classe di storage precedentemente configurata su tale cluster come classe di storage predefinita. Questa classe di storage verrà utilizzata quando non viene specificata alcuna classe di storage in una dichiarazione di volume persistente (PVC). La classe di storage predefinita può essere modificata in qualsiasi momento all'interno di Astra Control Center e qualsiasi classe di storage può essere utilizzata in qualsiasi momento specificando il nome della classe di storage all'interno del grafico PVC o Helm. Assicurarsi di avere definito solo una singola classe di storage predefinita per il cluster Kubernetes.

Per ulteriori informazioni

- "Documentazione di Astra Trident"

Ruoli e spazi dei nomi degli utenti

Scopri i ruoli e gli spazi dei nomi degli utenti in Astra Control e come utilizzarli per controllare l'accesso alle risorse della tua organizzazione.

Ruoli utente

È possibile utilizzare i ruoli per controllare l'accesso degli utenti alle risorse o alle funzionalità di Astra Control. Di seguito sono riportati i ruoli utente in Astra Control:

- Un **Viewer** può visualizzare le risorse.
- Un **Member** dispone delle autorizzazioni per il ruolo Viewer e può gestire app e cluster, annullare la gestione delle app ed eliminare snapshot e 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.

È possibile aggiungere vincoli a un utente membro o Viewer per limitare l'utente a uno o più utenti Spazi dei nomi.

Spazi dei nomi

Uno spazio dei nomi è un ambito che è possibile assegnare a risorse specifiche all'interno di un cluster gestito da Astra Control. Astra Control rileva gli spazi dei nomi di un cluster quando si aggiunge il cluster ad Astra Control. Una volta rilevati, gli spazi dei nomi sono disponibili per l'assegnazione come vincoli agli utenti. Solo i membri che hanno accesso a tale spazio dei nomi possono utilizzare tale risorsa. È possibile utilizzare gli spazi dei nomi per controllare l'accesso alle risorse utilizzando un paradigma adatto alla propria organizzazione, ad esempio per aree fisiche o divisioni all'interno di un'azienda. Quando si aggiungono vincoli a un utente, è possibile configurare tale utente in modo che abbia accesso a tutti gli spazi dei nomi o solo a un set specifico di spazi dei nomi. È inoltre possibile assegnare vincoli dello spazio dei nomi utilizzando le etichette dello spazio dei nomi.

Trova ulteriori informazioni

"Gestire utenti e ruoli locali"

Utilizzare Astra Control Center

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) e quindi andare alla pagina delle applicazioni in Astra Control per definire le applicazioni e le relative risorse.

Puoi definire e gestire le app che includono risorse storage con pod in esecuzione o app che includono risorse storage senza pod in esecuzione. Le app che non hanno pod in esecuzione sono note come applicazioni solo dati.

Requisiti di gestione delle applicazioni

Astra Control ha i seguenti requisiti di gestione delle applicazioni:

- **Licensing**: Per gestire le applicazioni utilizzando Astra Control Center, è necessaria la licenza di valutazione di Astra Control Center o una licenza completa.
- **Namespace**: Le applicazioni possono essere definite all'interno di uno o più namespace specificati su un singolo cluster utilizzando Astra Control. Un'applicazione può contenere risorse che spaziano da più spazi dei nomi all'interno dello stesso cluster. Astra Control non supporta la possibilità di definire le applicazioni in più cluster.
- **Storage class**: Se si installa un'applicazione con una classe di storage impostata in modo esplicito e si deve clonare l'applicazione, il cluster di destinazione per l'operazione di clone deve avere la classe di storage specificata in origine. La clonazione di un'applicazione con una classe di storage esplicitamente impostata su un cluster che non ha la stessa classe di storage non avrà esito positivo.
- **Kubernetes resources**: Le applicazioni che utilizzano risorse Kubernetes non raccolte da Astra Control potrebbero non disporre di funzionalità complete di gestione dei dati delle applicazioni. Astra Control raccoglie le seguenti risorse Kubernetes:

`ClusterRole`	`ClusterRoleBinding`	`ConfigMap`
`CronJob`	`CustomResourceDefinition`	`CustomResource`
`DaemonSet`	`DeploymentConfig`	`HorizontalPodAutoscaler`
`Ingress`	`MutatingWebhook`	`NetworkPolicy`
`PersistentVolumeClaim`	`Pod`	`PodDisruptionBudget`
`PodTemplate`	`ReplicaSet`	`Role`
`RoleBinding`	`Route`	`Secret`
`Service`	`ServiceAccount`	`StatefulSet`
`ValidatingWebhook`		

Metodi di installazione delle applicazioni supportati

Astra Control supporta i seguenti metodi di installazione dell'applicazione:

- **Manifest file**: Astra Control supporta le applicazioni installate da un file manifest utilizzando kubectl. Ad esempio:

```
kubectl apply -f myapp.yaml
```

- **Helm 3**: Se utilizzi Helm per installare le app, Astra Control richiede Helm versione 3. La gestione e la clonazione delle applicazioni installate con Helm 3 (o aggiornate da Helm 2 a Helm 3) sono completamente supportate. La gestione delle applicazioni installate con Helm 2 non è supportata.
- **Applicazioni distribuite dall'operatore**: Astra Control supporta le applicazioni installate con operatori con ambito namespace, in generale progettati con un'architettura "pass-by-value" piuttosto che "pass-by-reference". Un operatore e l'applicazione che installa devono utilizzare lo stesso namespace; potrebbe essere necessario modificare il file YAML di implementazione per l'operatore per garantire che ciò avvenga.

  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.

Installa le app sul tuo cluster

Dopo di che "aggiunto il cluster" In Astra Control, puoi installare le app o gestire quelle esistenti sul cluster. È possibile gestire qualsiasi applicazione con un ambito per uno o più spazi dei nomi.

Definire le applicazioni

Una volta che Astra Control rileva gli spazi dei nomi sui cluster, è possibile definire le applicazioni che si desidera gestire. È possibile scegliere gestisci un'applicazione che spazia uno o più spazi dei nomi oppure gestire un intero namespace come singola applicazione. Tutto questo si riduce al livello di granularità necessario per le operazioni di protezione dei dati.

Sebbene Astra Control ti consenta di gestire separatamente entrambi i livelli della gerarchia (lo spazio dei nomi e le applicazioni nello spazio dei nomi o negli spazi dei nomi), la Best practice 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.

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 come un'applicazione con un singolo spazio dei nomi.

Prima di iniziare

- Un cluster Kubernetes aggiunto ad Astra Control.
- Una o più applicazioni installate sul cluster. Scopri di più sui metodi di installazione delle app supportati.
- Spazi dei nomi esistenti nel cluster Kubernetes aggiunto ad Astra Control.
- (Facoltativo) un'etichetta Kubernetes su qualsiasi "Risorse Kubernetes supportate".

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".

A proposito di questa attività

- Prima di iniziare, dovresti anche capire "gestione degli spazi dei nomi standard e di sistema".
- Se intendi utilizzare più spazi dei nomi con le tue applicazioni in Astra Control, "modificare i ruoli utente con vincoli dello spazio dei nomi" Dopo l'aggiornamento a una versione di Astra Control Center con supporto di più namespace.
- Per istruzioni su come gestire le applicazioni utilizzando l'API Astra Control, vedere "Astra Automation e informazioni API".

Opzioni di gestione delle applicazioni

- Definire le risorse da gestire come applicazione
- Definire uno spazio dei nomi da gestire come applicazione

Definire le risorse da gestire come applicazione

È possibile specificare "Kubernetes risorse che compongono un'applicazione" Che si desidera gestire con Astra Control. La definizione di un'applicazione consente di raggruppare gli elementi del cluster Kubernetes in una singola applicazione. Questa raccolta di risorse Kubernetes è organizzata in base allo spazio dei nomi e ai criteri di selezione delle etichette.

La definizione di un'applicazione offre un controllo più granulare su ciò che deve essere incluso in un'operazione Astra Control, inclusi cloni, snapshot e backup.

Quando definisci le app, assicurati di non includere una risorsa Kubernetes in più app con policy di protezione. La sovrapposizione delle policy di protezione sulle risorse Kubernetes può causare conflitti di dati. Scopri di più in un esempio.

Espandi per ulteriori informazioni sull'aggiunta di risorse con ambito cluster agli spazi dei nomi delle app.

È possibile importare risorse del cluster associate alle risorse dello spazio dei nomi oltre a quelle incluse automaticamente in Astra Control. È possibile aggiungere una regola che includerà le risorse di un gruppo specifico, un tipo, una versione e, facoltativamente, un'etichetta. Questa operazione potrebbe essere utile se ci sono risorse che Astra Control non include automaticamente.

Non è possibile escludere nessuna delle risorse con ambito del cluster incluse automaticamente da Astra Control.

È possibile aggiungere quanto segue `apiVersions` (Che sono i gruppi combinati con la versione API):

Tipo di risorsa	ApiVersions (gruppo + versione)
`ClusterRole`	rbac.authorization.k8s.io/v1
`ClusterRoleBinding`	rbac.authorization.k8s.io/v1
`CustomResource`	apiextensions.k8s.io/v1, apiextensions.k8s.io/v1beta1
`CustomResourceDefinition`	apiextensions.k8s.io/v1, apiextensions.k8s.io/v1beta1
`MutatingWebhookConfiguration`	admissionregistration.k8s.io/v1
`ValidatingWebhookConfiguration`	admissionregistration.k8s.io/v1

Fasi

1. Dalla pagina applicazioni, selezionare **Definisci**.
2. Nella finestra **define application** (Definisci applicazione), inserire il nome dell'applicazione.
3. Scegliere il cluster in cui viene eseguita l'applicazione nell'elenco a discesa **Cluster**.
4. Scegliere uno spazio dei nomi per l'applicazione dall'elenco a discesa **namespace**.

   Le applicazioni possono essere definite all'interno di uno o più spazi dei nomi specifici su un singolo cluster utilizzando Astra Control. Un'applicazione può contenere risorse che spaziano da più spazi dei nomi all'interno dello stesso cluster. Astra Control non supporta la possibilità di definire le applicazioni in più cluster.

5. (Facoltativo) inserire un'etichetta per le risorse Kubernetes in ogni namespace. È possibile specificare un'etichetta singola o criteri di selezione delle etichette (query).

   Per ulteriori informazioni sulle etichette Kubernetes, "Consulta la documentazione ufficiale di Kubernetes".

6. (Facoltativo) aggiungere spazi dei nomi aggiuntivi per l'applicazione selezionando **Aggiungi spazio dei nomi** e scegliendo lo spazio dei nomi dall'elenco a discesa.
7. (Facoltativo) inserire i criteri di selezione di un'etichetta o di un'etichetta singola per gli spazi dei nomi aggiuntivi aggiunti.
8. (Facoltativo) per includere risorse con ambito cluster oltre a quelle incluse automaticamente da Astra Control, selezionare **Includi risorse aggiuntive con ambito cluster** e completare quanto segue:

a. Selezionare **Aggiungi regola di inclusione**.
b. **Gruppo**: Selezionare il gruppo di risorse API dall'elenco a discesa.
c. **Kind**: Dall'elenco a discesa, selezionare il nome dello schema dell'oggetto.
d. **Version**: Inserire la versione dell'API.
e. **Selettore etichetta**: Facoltativamente, includere un'etichetta da aggiungere alla regola. Questa etichetta viene utilizzata per recuperare solo le risorse corrispondenti a questa etichetta. Se non si fornisce un'etichetta, Astra Control raccoglie tutte le istanze del tipo di risorsa specificato per quel cluster.
f. Esaminare la regola creata in base alle voci immesse.
g. Selezionare **Aggiungi**.

È possibile creare tutte le regole di risorse con ambito cluster desiderate. Le regole vengono visualizzate nel riepilogo dell'applicazione Definisci.

9. Selezionare **Definisci**.
10. Dopo aver selezionato **define**, ripetere la procedura per altre applicazioni, in base alle necessità.

Al termine della definizione di un'applicazione, l'applicazione viene visualizzata in `Healthy` indicare nell'elenco delle applicazioni nella pagina applicazioni. Ora è possibile clonarlo e creare backup e snapshot.

L'applicazione appena aggiunta potrebbe presentare 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.

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

Per visualizzare le risorse aggiunte a questa applicazione, selezionare la scheda **risorse**. Selezionare il numero dopo il nome della risorsa nella colonna Resource (risorsa) o inserire il nome della risorsa nella Search (Cerca) per visualizzare le risorse aggiuntive incluse nell'ambito del cluster.

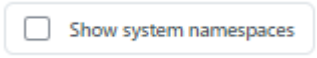
Definire uno spazio dei nomi da gestire come applicazione

È possibile aggiungere tutte le risorse Kubernetes in uno spazio dei nomi alla gestione di Astra Control definendo le risorse dello spazio dei nomi come applicazione. Questo metodo è preferibile alla definizione individuale delle applicazioni se si intende gestire e proteggere tutte le risorse in un determinato namespace in modo simile e a intervalli comuni.

Fasi

1. Dalla pagina Clusters, selezionare un cluster.
2. Selezionare la scheda **spazi dei nomi**.
3. Selezionare il menu Actions (azioni) per lo spazio dei nomi che contiene le risorse dell'applicazione che si desidera gestire e selezionare **define as application** (Definisci come applicazione).

Se si desidera definire più applicazioni, selezionare dall'elenco namespace e selezionare il pulsante **azioni** nell'angolo in alto a sinistra, quindi selezionare **Definisci come applicazione**. In questo modo verranno definite più applicazioni singole nei rispettivi spazi dei nomi. Per le applicazioni con più spazi dei nomi, vedere Definire le risorse da gestire come applicazione.

Selezionare la casella di controllo **Show system namespace** (Mostra spazi dei nomi di sistema) per visualizzare gli spazi dei nomi di sistema solitamente non utilizzati nella gestione delle applicazioni per impostazione predefinita. 

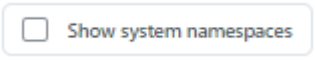
"Scopri di più".

Al termine del processo, le applicazioni associate allo spazio dei nomi vengono visualizzate in `Associated applications` colonna.

E gli spazi dei nomi di sistema?

Astra Control rileva anche gli spazi dei nomi di sistema su un cluster Kubernetes. Per impostazione predefinita, questi spazi dei nomi di sistema non vengono visualizzati perché è raro che sia necessario eseguire il backup delle risorse delle applicazioni di sistema.

È possibile visualizzare gli spazi dei nomi di sistema dalla scheda spazi dei nomi di un cluster selezionato selezionando la casella di controllo **Mostra spazi dei nomi di sistema**.



Per impostazione predefinita, Astra Control Center non viene visualizzato come applicazione gestibile, ma è possibile eseguire il backup e il ripristino di un'istanza di Astra Control Center utilizzando un'altra istanza di Astra Control Center.

Esempio: Policy di protezione separata per release diverse

In questo esempio, il team devops sta gestendo un'implementazione di release "canary". Il cluster del team 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: Una per la release "canary" e una per la release "stable". In questo modo i backup, gli snapshot e le operazioni di clonazione vengono separati per i due gruppi di oggetti Kubernetes.

Trova ulteriori informazioni

- "Utilizzare l'API di controllo Astra"
- "Annullare la gestione di un'applicazione"

Proteggi le app

Panoramica della protezione

Con Astra Control Center puoi creare backup, cloni, snapshot e policy di protezione per le tue applicazioni. Il backup delle tue applicazioni aiuta i tuoi servizi e i dati associati a essere il più possibile disponibili; durante uno scenario di disastro, il ripristino dal backup può garantire il ripristino completo di un'applicazione e dei dati associati con interruzioni minime. Backup, cloni e snapshot possono contribuire a proteggere da minacce comuni come ransomware, perdita accidentale di dati e disastri ambientali. "Scopri i tipi di protezione dei dati disponibili in Astra Control Center e quando utilizzarli".

Inoltre, è possibile replicare le applicazioni in un cluster remoto in preparazione del disaster recovery.

Workflow di protezione delle app

Puoi utilizzare il seguente flusso di lavoro di esempio per iniziare a proteggere le tue applicazioni.

[Uno] Proteggi tutte le app

Per garantire la protezione immediata delle applicazioni, "creare un backup manuale di tutte le applicazioni".

[Due] Configurare una policy di protezione per ogni applicazione

Per automatizzare backup e snapshot futuri, "configurare una policy di protezione per ogni applicazione". Ad esempio, è possibile iniziare con backup settimanali e snapshot giornalieri, con un mese di conservazione per entrambi. Si consiglia vivamente di automatizzare backup e snapshot con una policy di protezione rispetto a backup e snapshot manuali.

[Tre] Modificare i criteri di protezione

Man mano che le applicazioni e i loro modelli di utilizzo cambiano, regola le policy di protezione in base alle necessità per fornire la migliore protezione.

[Quattro] Replica delle applicazioni su un cluster remoto

"Replicare le applicazioni" A un cluster remoto utilizzando la tecnologia SnapMirror di NetApp. Astra Control replica le snapshot su un cluster remoto, offrendo funzionalità di disaster recovery asincrone.

[Cinque] In caso di disastro, ripristinate le applicazioni con il backup o la replica più recente sul sistema remoto

In caso di perdita di dati, è possibile eseguire il ripristino "ripristino del backup più recente" primo per ogni applicazione. È quindi possibile ripristinare l'ultimo snapshot (se disponibile). In alternativa, è possibile utilizzare la replica su un sistema remoto.

Proteggi le app con snapshot e backup

Proteggi tutte le app eseguendo snapshot e backup utilizzando una policy di protezione automatica o ad-hoc. È possibile utilizzare l'interfaccia utente di Astra Control Center o. "L'API Astra Control" per proteggere le applicazioni.

A proposito di questa attività

- **Helm ha implementato le app**: 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.

- **(solo cluster OpenShift) Aggiungi criteri**: Quando si crea un progetto per ospitare un'app su un cluster OpenShift, al progetto (o spazio dei nomi 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
```

È possibile eseguire le seguenti attività relative alla protezione dei dati dell'applicazione:

- Configurare un criterio di protezione
- Creare un'istantanea
- Creare un backup
- Abilita backup e ripristino per le operazioni economiche a ontap-nas
- Creare un backup immutabile
- Visualizzare snapshot e backup
- Eliminare le istantanee
- Annullare i backup
- Eliminare i backup

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.

Se hai bisogno di backup o snapshot per eseguire più frequentemente di una volta all'ora, è possibile "Utilizza l'API REST di Astra Control per creare snapshot e backup".

Se si sta definendo un criterio di protezione che crea backup immutabili per bucket WORM (Write Once Read Many), assicurarsi che il tempo di conservazione per i backup non sia inferiore al periodo di conservazione configurato per il bucket.

Eseguire l'offset delle pianificazioni di backup e replica per evitare sovrapposizioni di pianificazione. Ad esempio, eseguire backup all'inizio dell'ora ogni ora e pianificare la replica per iniziare con un offset di 5 minuti e un intervallo di 10 minuti.

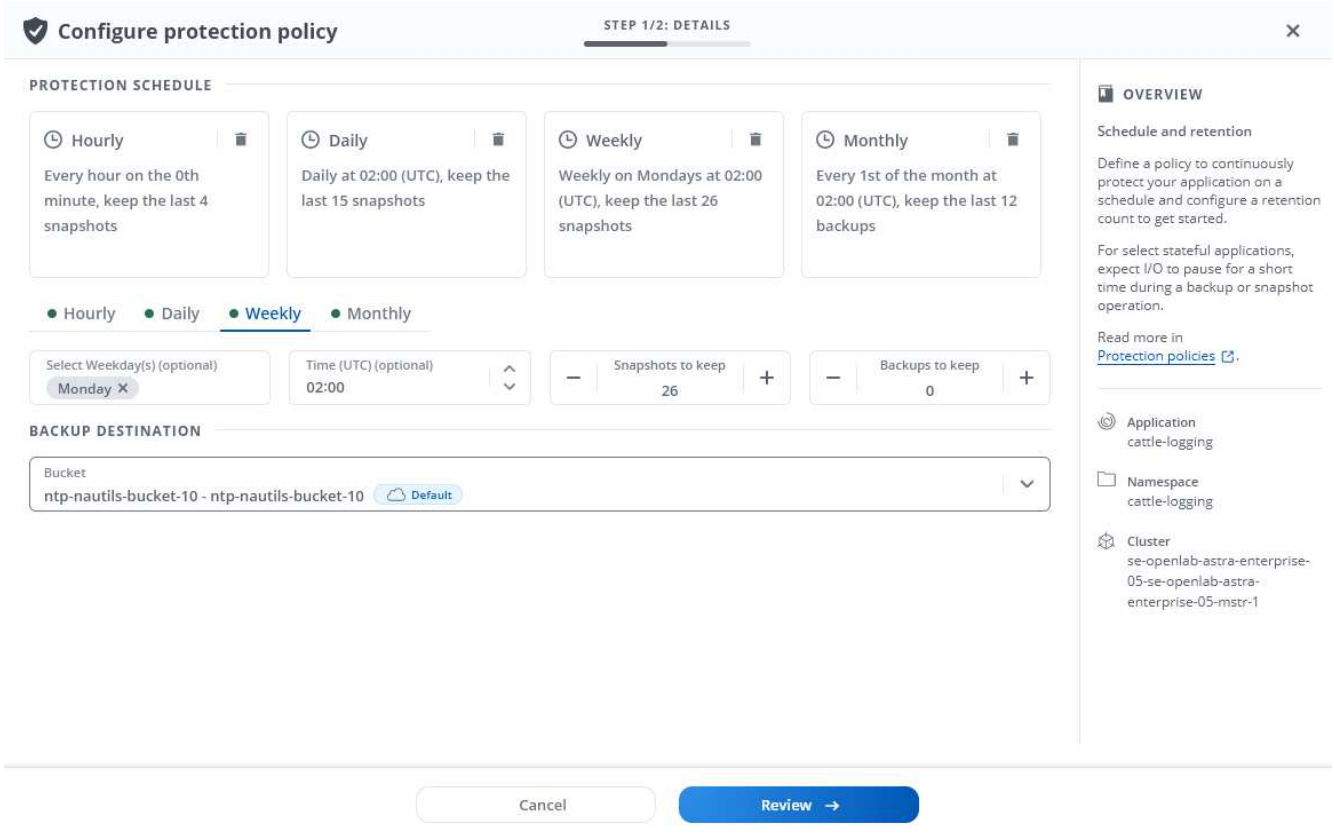
Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Selezionare **Data Protection** (protezione dati).
3. Selezionare **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.

Quando si imposta un livello di conservazione per i backup, è possibile scegliere il bucket in cui si desidera memorizzare i backup.

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



5. Selezionare **Revisione**.
6. Selezionare **Imposta policy di protezione.**

Risultato

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

Creare un'istantanea

Puoi creare uno snapshot on-demand in qualsiasi momento.

A proposito di questa attività

Astra Control supporta la creazione di snapshot utilizzando classi di storage supportate dai seguenti driver:

- `ontap-nas`
- `ontap-san`
- `ontap-san-economy`

Se l'applicazione utilizza una classe di storage supportata da `ontap-nas-economy` driver, impossibile creare snapshot. Utilizzare una classe di storage alternativa per gli snapshot.

Fasi

1. Selezionare **applicazioni**.
2. Dal menu Options (Opzioni) nella colonna **Actions** (azioni) dell'applicazione desiderata, selezionare **Snapshot**.
3. Personalizzare il nome dell'istantanea, quindi selezionare **Avanti**.
4. Esaminare il riepilogo dell'istantanea e selezionare **Snapshot**.

Risultato

Viene avviato il processo di snapshot. Un'istantanea ha successo quando lo stato è **integro** nella colonna **Stato** della pagina **Data Protection** > **Snapshot**.

Creare un backup

Puoi eseguire il backup di un'app in qualsiasi momento.

A proposito di questa attività

I bucket in Astra Control non riportano la capacità disponibile. Prima di eseguire il backup o il cloning delle applicazioni gestite da Astra Control, controllare le informazioni del bucket nel sistema di gestione dello storage appropriato.

Se l'applicazione utilizza una classe di storage supportata da `ontap-nas-economy` driver, è necessario attivare il backup e il ripristino funzionalità. Accertarsi di aver definito un `backendType` nel "Oggetto storage Kubernetes" con un valore di `ontap-nas-economy` prima di eseguire qualsiasi operazione di protezione.

Astra Control supporta la creazione di backup utilizzando classi di storage supportate dai seguenti driver:

- `ontap-nas`
- `ontap-nas-economy`
- `ontap-san`
- `ontap-san-economy`

Fasi

1. Selezionare **applicazioni**.
2. Dal menu Opzioni nella colonna **azioni** dell'applicazione desiderata, selezionare **Backup**.
3. Personalizzare il nome del backup.
4. 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.
5. Scegliere un bucket di destinazione per il backup dall'elenco dei bucket di storage.
6. Selezionare **Avanti**.
7. Esaminare il riepilogo del backup e selezionare **Backup**.

Risultato

Astra Control 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.
- Per annullare un backup in esecuzione, seguire le istruzioni riportate in Annullare i backup. Per eliminare il backup, attendere il completamento, quindi seguire le istruzioni riportate in Eliminare i backup.
- 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.

Abilita backup e ripristino per le operazioni economiche a ontap-nas

Astra Control Provivisioner fornisce funzionalità di backup e ripristino che possono essere abilitate per i backend di storage che stanno utilizzando `ontap-nas-economy` classe di storage.

Prima di iniziare

- Lo hai fatto "Abilitato Astra Control Provisioner".
- Hai definito un'applicazione in Astra Control. Questa applicazione dispone di funzionalità di protezione limitate fino al completamento di questa procedura.
- Lo hai fatto `ontap-nas-economy` selezionata come classe di archiviazione predefinita per il backend di archiviazione.

Espandere per la procedura di configurazione

1. Sul back-end dello storage ONTAP:

   a. Trova la SVM che ospita `ontap-nas-economy`volumi basati su -dell'applicazione.

   b. Accedere a un terminale connesso a ONTAP in cui vengono creati i volumi.

   c. Nascondi la directory snapshot per la SVM:

   > Questo cambiamento influisce sull'intera SVM. La directory nascosta continuerà ad essere accessibile.

   ```
   nfs modify -vserver <svm name> -v3-hide-snapshot enabled
   ```

   +

   > Verificare che la directory snapshot sul backend di archiviazione ONTAP sia nascosta. La mancata visualizzazione di questa directory potrebbe causare la perdita di accesso all'applicazione, in particolare se si utilizza NFSv3.

2. In Astra Trident:

   a. Abilitare la directory snapshot per ogni PV `ontap-nas-economy` basato e associato all'applicazione:

   ```
   tridentctl update volume <pv name> --snapshot-dir=true --pool
   -level=true -n trident
   ```

   b. Confermare che la directory snapshot è stata abilitata per ogni PV associato:

   ```
   tridentctl get volume <pv name> -n trident -o yaml | grep
   snapshotDir
   ```

   Risposta:

   ```
   snapshotDirectory: "true"
   ```

3. In Astra Control, aggiorna l'applicazione dopo aver abilitato tutte le directory di snapshot associate, in modo che Astra Control riconosca il valore modificato.

Risultato

L'applicazione è pronta per il backup e il ripristino utilizzando Astra Control. Ciascun PVC è inoltre disponibile per essere utilizzato da altre applicazioni per backup e ripristini.

Creare un backup immutabile

Un backup immutabile non può essere modificato, eliminato o sovrascritto se la politica di conservazione nel bucket che archivia il backup lo vieta. Puoi creare backup immutabili eseguendo il backup delle applicazioni in bucket che hanno configurato un criterio di conservazione. Fare riferimento a. "Protezione dei dati" per informazioni importanti sull'utilizzo dei backup immutabili.

Prima di iniziare

È necessario configurare il bucket di destinazione con un criterio di conservazione. La scelta varia in base al provider di storage utilizzato. Per ulteriori informazioni, consultare la documentazione del provider di storage:

- **Amazon Web Services**: "Abilitare il blocco degli oggetti S3 durante la creazione del bucket e impostare una modalità di conservazione predefinita di "governance" con un periodo di conservazione predefinito".
- **NetApp StorageGRID**: "Abilitare blocco oggetto S3 durante la creazione del bucket e impostare una modalità di conservazione predefinita di "conformità" con un periodo di conservazione predefinito".

> I bucket in Astra Control non riportano la capacità disponibile. Prima di eseguire il backup o il cloning delle applicazioni gestite da Astra Control, controllare le informazioni del bucket nel sistema di gestione dello storage appropriato.

> Se l'applicazione utilizza una classe di storage supportata da `ontap-nas-economy` driver, assicurarsi di aver definito un `backendType` nel "Oggetto storage Kubernetes" con un valore di `ontap-nas-economy` prima di eseguire qualsiasi operazione di protezione.

Fasi

1. Selezionare **applicazioni**.
2. Dal menu Opzioni nella colonna **azioni** dell'applicazione desiderata, selezionare **Backup**.
3. Personalizzare il nome del backup.
4. 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.
5. Scegliere un bucket di destinazione per il backup dall'elenco dei bucket di storage. Un bucket WORM (Write Once Read Many) viene indicato con lo stato "bloccato" accanto al nome del bucket.

   > Se la benna è di tipo non supportato, ciò viene indicato quando si passa il mouse o si seleziona la benna.

6. Selezionare **Avanti**.
7. Esaminare il riepilogo del backup e selezionare **Backup**.

Risultato

Astra Control crea un backup immutabile dell'app.

- 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.
- Se provi a creare due backup immutabili della stessa app nello stesso bucket contemporaneamente, Astra Control impedisce l'avvio del secondo backup. Attendere il completamento del primo backup prima di avviarne un altro.
- Non è possibile annullare un backup immutabile in esecuzione.
- 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).

Un backup immutabile viene indicato con lo stato "bloccato" accanto al bucket in uso.

Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Selezionare **Data Protection** (protezione dati).

   Le istantanee vengono visualizzate per impostazione predefinita.
3. Selezionare **Backup** per visualizzare l'elenco dei backup.

Eliminare le istantanee

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

Non è possibile eliminare uno snapshot attualmente in fase di replica.

Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione gestita.
2. Selezionare **Data Protection** (protezione dati).
3. Dal menu Options (Opzioni) nella colonna **Actions** (azioni) per lo snapshot desiderato, selezionare **Delete snapshot** (Elimina snapshot).
4. Digitare la parola "DELETE" per confermare l'eliminazione, quindi selezionare **Yes, Delete snapshot**.

Risultato

Astra Control elimina lo snapshot.

Annullare i backup

È possibile annullare un backup in corso.

Per annullare un backup, il backup deve essere in `Running` stato. Non è possibile annullare un backup in `Pending` stato.

Non è possibile annullare un backup immutabile in esecuzione.

Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Selezionare **Data Protection** (protezione dati).
3. Selezionare **Backup**.
4. Dal menu Options (Opzioni) nella colonna **Actions** (azioni) per il backup desiderato, selezionare **Cancel** (Annulla).
5. Digitare la parola "CANCEL" per confermare l'operazione, quindi selezionare **Yes, CANCEL backup** (Sì, Annulla backup*).

Eliminare i backup

Eliminare i backup pianificati o on-demand non più necessari. Non è possibile eliminare un backup eseguito in un bucket immutabile finché il criterio di conservazione del bucket non lo consente.

Non è possibile eliminare un backup immutabile prima della scadenza del periodo di conservazione.

Per annullare un backup in esecuzione, seguire le istruzioni riportate in Annullare i backup. Per eliminare il backup, attendere che sia stato completato, quindi seguire queste istruzioni.

Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Selezionare **Data Protection** (protezione dati).
3. Selezionare **Backup**.
4. Dal menu Options (Opzioni) nella colonna **Actions** (azioni) per il backup desiderato, selezionare **Delete backup** (Elimina backup).
5. Digitare la parola "DELETE" per confermare l'eliminazione, quindi selezionare **Yes, Delete backup**.

Risultato

Astra Control elimina il backup.

Ripristinare le applicazioni

Astra Control può ripristinare l'applicazione da uno snapshot o da un backup. Il ripristino da uno snapshot esistente sarà più rapido quando si ripristina l'applicazione nello stesso cluster. È possibile utilizzare l'interfaccia utente di Astra Control o. "API di controllo Astra" per ripristinare le applicazioni.

Prima di iniziare

- **Proteggi prima le tue applicazioni**: Ti consigliamo vivamente di creare un'istantanea o un backup dell'applicazione prima di ripristinarla. Ciò consente di clonare dallo snapshot o dal backup se il ripristino

non ha avuto esito positivo.

- **Check destination Volumes** (Controlla volumi di destinazione): Se si esegue il ripristino in una classe di storage diversa, assicurarsi che la classe di storage 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. Ad esempio, se il volume persistente di origine utilizza la modalità di accesso RWX, selezionare una classe di storage di destinazione che non è in grado di fornire RWX, come Azure Managed Disks, AWS EBS, Google Persistent Disk o. `ontap-san`, causa l'errore dell'operazione di ripristino. Per ulteriori informazioni sulle modalità di accesso al volume persistente, fare riferimento a. "Kubernetes" documentazione.
- **Pianificare le esigenze di spazio**: Quando si esegue un ripristino in-place di un'applicazione che utilizza lo storage NetApp ONTAP, lo spazio utilizzato dall'applicazione ripristinata può raddoppiare. Dopo aver eseguito un ripristino in-place, rimuovere eventuali snapshot indesiderati dall'applicazione ripristinata per liberare spazio di storage.
- **(solo cluster Red Hat OpenShift) Aggiungi criteri**: Quando si crea un progetto per ospitare un'app su un cluster OpenShift, al progetto (o spazio dei nomi 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
```

- **Driver di classe di archiviazione supportati**: Astra Control supporta il ripristino dei backup utilizzando classi di archiviazione supportate dai seguenti driver:
  - `ontap-nas`
  - `ontap-nas-economy`
  - `ontap-san`
  - `ontap-san-economy`
- * (Solo driver ontap-nas-Economy) esegue backup e ripristini*: Prima di eseguire il backup o il ripristino di un'app che utilizza una classe di storage supportata da `ontap-nas-economy` driver, verificare che "La directory snapshot sul backend dello storage ONTAP è nascosta". La mancata visualizzazione di questa directory potrebbe causare la perdita di accesso all'applicazione, in particolare se si utilizza NFSv3.
- **Helm ha implementato le applicazioni**: Le 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.

> L'esecuzione di un'operazione di ripristino in-place su un'applicazione che condivida le risorse con un'altra applicazione può avere risultati non intenzionale. Tutte le risorse condivise tra le applicazioni vengono sostituite quando viene eseguito un ripristino in-place su una delle applicazioni. Per ulteriori informazioni, vedere questo esempio.

Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Dal menu Opzioni nella colonna azioni, selezionare **Ripristina**.
3. Scegliere il tipo di ripristino:
   - **Ripristina gli spazi dei nomi originali**: Utilizzare questa procedura per ripristinare l'applicazione sul

posto nel cluster originale.

> Se l'applicazione utilizza una classe di storage supportata da `ontap-nas-economy` driver, è necessario ripristinare l'applicazione utilizzando le classi di storage originali. Non è possibile specificare un'altra classe di storage se si ripristina l'applicazione nello stesso namespace.

i. Seleziona lo snapshot o il backup da utilizzare per ripristinare l'applicazione in-place, che ripristina l'applicazione a una versione precedente di se stessa.

ii. Selezionare **Avanti**.

> Se si ripristina uno spazio dei nomi precedentemente cancellato, viene creato un nuovo spazio dei nomi con lo stesso nome come parte del processo di ripristino. Tutti gli utenti che disponevano dei diritti per gestire le applicazioni nello spazio dei nomi precedentemente cancellato devono ripristinare manualmente i diritti nello spazio dei nomi appena ricreato.

◦ **Ripristina nuovi spazi dei nomi**: Utilizzare questa procedura per ripristinare l'applicazione in un altro cluster o con spazi dei nomi diversi dall'origine.

i. Specificare il nome dell'applicazione ripristinata.

ii. Scegliere il cluster di destinazione per l'applicazione che si desidera ripristinare.

iii. Immettere uno spazio dei nomi di destinazione per ogni spazio dei nomi di origine associato all'applicazione.

> Astra Control crea nuovi spazi dei nomi di destinazione come parte di questa opzione di ripristino. Gli spazi dei nomi di destinazione specificati non devono essere già presenti nel cluster di destinazione.

iv. Selezionare **Avanti**.

v. Selezionare lo snapshot o il backup da utilizzare per ripristinare l'applicazione.

vi. Selezionare **Avanti**.

vii. Scegliere una delle seguenti opzioni:

- **Ripristina utilizzando le classi di storage originali**: L'applicazione utilizza la classe di storage originariamente associata, a meno che non esista nel cluster di destinazione. In questo caso, viene utilizzata la classe di storage predefinita per il cluster.
- **Ripristinare utilizzando una classe di storage diversa**: Selezionare una classe di storage esistente nel cluster di destinazione. Tutti i volumi delle applicazioni, indipendentemente dalle classi di storage originariamente associate, verranno migrati in questa diversa classe di storage come parte del ripristino.

viii. Selezionare **Avanti**.

4. Scegli le risorse da filtrare:

◦ **Restore all resources** (Ripristina tutte le risorse): Ripristina tutte le risorse associate all'applicazione originale.

◦ **Filter resources**: Specificare le regole per ripristinare un sottoinsieme delle risorse applicative originali:

i. Scegliere di includere o escludere risorse dall'applicazione ripristinata.

ii. Selezionare **Aggiungi regola di inclusione** o **Aggiungi regola di esclusione** e configurare la regola per filtrare le risorse corrette durante il ripristino dell'applicazione. È possibile modificare una regola o rimuoverla e crearne di nuovo fino a quando la configurazione non è corretta.

> Per ulteriori informazioni sulla configurazione delle regole di inclusione ed esclusione, vedere Filtrare le risorse durante il ripristino di un'applicazione.

5. Selezionare **Avanti**.
6. Esaminare attentamente i dettagli relativi all'azione di ripristino, digitare "restore" (se richiesto) e selezionare **Restore**.

Risultato

Astra Control ripristina l'applicazione in base alle informazioni fornite. Se hai ripristinato l'applicazione in-place, il contenuto dei volumi persistenti esistenti viene sostituito con il contenuto dei volumi persistenti dell'applicazione ripristinata.

> Dopo un'operazione di protezione dei dati (cloning, backup o ripristino) e il successivo ridimensionamento persistente del volume, si verifica un ritardo fino a venti minuti prima che la nuova dimensione del volume venga visualizzata nell'interfaccia utente Web. 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.

> Qualsiasi utente membro con vincoli di spazio dei nomi in base al nome/ID dello spazio dei nomi o alle etichette dello spazio dei nomi può clonare o ripristinare un'applicazione in un nuovo spazio dei nomi nello stesso cluster o in qualsiasi altro cluster dell'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 l'account utente membro e aggiornare i vincoli di ruolo affinché l'utente interessato conceda l'accesso al nuovo spazio dei nomi.

Filtrare le risorse durante il ripristino di un'applicazione

È possibile aggiungere una regola di filtro a un "ripristinare" operazione che specifica le risorse applicative esistenti da includere o escludere dall'applicazione ripristinata. È possibile includere o escludere risorse in base a uno spazio dei nomi, un'etichetta o un GVK (GroupVersionKind) specificati.

Espandere per ulteriori informazioni sugli scenari di inclusione ed esclusione

- **Si seleziona una regola di inclusione con spazi dei nomi originali (ripristino in-place)**: Le risorse applicative esistenti definite nella regola verranno eliminate e sostituite da quelle dello snapshot o del backup selezionato che si sta utilizzando per il ripristino. Tutte le risorse non specificate nella regola di inclusione resteranno invariate.
- **Selezionare una regola di inclusione con nuovi spazi dei nomi**: Utilizzare la regola per selezionare le risorse specifiche che si desidera utilizzare nell'applicazione ripristinata. Le risorse non specificate nella regola di inclusione non verranno incluse nell'applicazione ripristinata.
- **Si seleziona una regola di esclusione con spazi dei nomi originali (ripristino in-place)**: Le risorse specificate per l'esclusione non verranno ripristinate e rimarranno invariate. Le risorse non specificate da escludere verranno ripristinate dallo snapshot o dal backup. Tutti i dati sui volumi persistenti verranno cancellati e ricreati se il corrispondente StatefulSet fa parte delle risorse filtrate.
- **Selezionare una regola di esclusione con nuovi spazi dei nomi**: Utilizzare la regola per selezionare le risorse specifiche che si desidera rimuovere dall'applicazione ripristinata. Le risorse non specificate da escludere verranno ripristinate dallo snapshot o dal backup.

Le regole possono includere o escludere tipi. Non sono disponibili regole che combinano inclusione ed esclusione delle risorse.

Fasi

1. Dopo aver scelto di filtrare le risorse e aver selezionato un'opzione di inclusione o esclusione nella procedura guidata Restore App, selezionare **Aggiungi regola di inclusione** o **Aggiungi regola di esclusione**.

   Non è possibile escludere risorse con ambito cluster che vengono automaticamente incluse da Astra Control.

2. Configurare la regola di filtro:

   È necessario specificare almeno uno spazio dei nomi, un'etichetta o un GVK. Assicurarsi che tutte le risorse conservate dopo l'applicazione delle regole di filtro siano sufficienti per mantenere l'applicazione ripristinata in uno stato di integrità.

   a. Selezionare uno spazio dei nomi specifico per la regola. Se non si effettua una selezione, nel filtro verranno utilizzati tutti gli spazi dei nomi.

      Se l'applicazione conteneva originariamente più spazi dei nomi e la ripristinerai in nuovi spazi dei nomi, tutti gli spazi dei nomi verranno creati anche se non contengono risorse.

   b. (Facoltativo) inserire un nome di risorsa.

   c. (Facoltativo) **selettore di etichette**: Includere un "selettore di etichette" da aggiungere alla regola. Il selettore di etichette viene utilizzato per filtrare solo le risorse corrispondenti all'etichetta selezionata.

   d. (Facoltativo) selezionare **Use GVK (GroupVersionKind) set to filter resources** for additional filtering options.

      Se si utilizza un filtro GVK, è necessario specificare versione e tipo.

      i. (Facoltativo) **Group**: Dall'elenco a discesa, selezionare il gruppo Kubernetes API.

ii. **Kind**: Dall'elenco a discesa, selezionare lo schema dell'oggetto per il tipo di risorsa Kubernetes da utilizzare nel filtro.

iii. **Version** (versione): Selezionare la versione dell'API Kubernetes.

3. Esaminare la regola creata in base alle voci immesse.
4. Selezionare **Aggiungi**.

È possibile creare tutte le regole di inclusione ed esclusione delle risorse desiderate. Le regole vengono visualizzate nel riepilogo dell'applicazione di ripristino prima di avviare l'operazione.

Problemi di ripristino in-place per un'applicazione che condivide le risorse con un'altra applicazione

È possibile eseguire un'operazione di ripristino in-place su un'applicazione che condivide le risorse con un'altra applicazione e produce risultati non desiderati. Tutte le risorse condivise tra le applicazioni vengono sostituite quando viene eseguito un ripristino in-place su una delle applicazioni.

Di seguito viene riportato uno scenario di esempio che crea una situazione indesiderabile quando si utilizza la replica di NetApp SnapMirror per un ripristino:

1. L'applicazione viene definita `app1` utilizzo dello spazio dei nomi `ns1`.
2. Viene configurata una relazione di replica per `app1`.
3. L'applicazione viene definita `app2` (sullo stesso cluster) utilizzando gli spazi dei nomi `ns1` e. `ns2`.
4. Viene configurata una relazione di replica per `app2`.
5. La replica inversa per `app2`. Questo causa il `app1` app sul cluster di origine da disattivare.

Replica delle applicazioni tra back-end di storage utilizzando la tecnologia SnapMirror

Grazie ad Astra Control, puoi creare business continuity per le tue applicazioni con un RPO (Recovery Point Objective) basso e un RTO basso (Recovery Time Objective) utilizzando le funzionalità di replica asincrona della tecnologia NetApp SnapMirror. Una volta configurata, questa opzione consente alle applicazioni di replicare le modifiche dei dati e delle applicazioni da un backend di storage all'altro, sullo stesso cluster o tra cluster diversi.

Per un confronto tra backup/ripristini e replica, fare riferimento a. "Concetti relativi alla protezione dei dati".

Puoi replicare le app in diversi scenari, come ad esempio i seguenti scenari on-premise, ibridi e multi-cloud:

- Dal sito a on-premise al sito A on-premise
- Dal sito a on-premise al sito B on-premise
- On-premise per il cloud con Cloud Volumes ONTAP
- Cloud con Cloud Volumes ONTAP in on-premise
- Cloud con Cloud Volumes ONTAP al cloud (tra diverse regioni dello stesso cloud provider o a diversi cloud provider)

Astra Control è in grado di replicare le applicazioni tra cluster on-premise, on-premise nel cloud (utilizzando Cloud Volumes ONTAP) o tra cloud (da Cloud Volumes ONTAP a Cloud Volumes ONTAP).

> È possibile replicare contemporaneamente un'altra applicazione nella direzione opposta. Ad esempio, è possibile replicare le applicazioni A, B, C dal Datacenter 1 al Datacenter 2 e le applicazioni X, Y, Z dal Datacenter 2 al Datacenter 1.

Utilizzando Astra Control, è possibile eseguire le seguenti attività relative alla replica delle applicazioni:

- Impostare una relazione di replica
- Portare online un'applicazione replicata sul cluster di destinazione (failover)
- Risincronizzare una replica con esito negativo
- Replica inversa delle applicazioni
- Eseguire il failback delle applicazioni nel cluster di origine originale
- Eliminare una relazione di replica dell'applicazione

Prerequisiti per la replica

La replica dell'applicazione Astra Control richiede che i seguenti prerequisiti siano soddisfatti prima di iniziare:

Cluster ONTAP

- * Astra Trident*: Astra Trident versione 22.10 o successiva deve esistere sia sui cluster Kubernetes di origine che di destinazione che utilizzano ONTAP come backend. Astra Control supporta la replica con la tecnologia NetApp SnapMirror utilizzando classi di storage supportate dai seguenti driver:
  - `ontap-nas`
  - `ontap-san`
- **Licenze**: Le licenze asincrone di ONTAP SnapMirror che utilizzano il bundle di protezione dati devono essere attivate sia sul cluster ONTAP di origine che su quello di destinazione. Fare riferimento a. "Panoramica sulle licenze SnapMirror in ONTAP" per ulteriori informazioni.

Peering

- **Cluster e SVM**: I backend dello storage ONTAP devono essere peering. Fare riferimento a. "Panoramica del peering di cluster e SVM" per ulteriori informazioni.

  > Assicurati che i nomi delle SVM utilizzati nella relazione di replica tra due cluster ONTAP siano univoci.

- * Astra Trident e SVM*: Le SVM remote con peering devono essere disponibili per Astra Trident sul cluster di destinazione.

Centro di controllo Astra

- **Backend gestiti**: È necessario aggiungere e gestire i backend di storage ONTAP in Astra Control Center per creare una relazione di replica.

  solo per Astra Control Provisioner: L'aggiunta e la gestione di backend di storage ONTAP in Astra Control Center è opzionale se hai abilitato Astra Control Provisioner per Astra Control Center 23,10 o versioni successive.

- **Cluster gestiti**: Aggiungere e gestire i seguenti cluster con Astra Control, idealmente in diversi domini o

siti di errore:

  - Cluster Kubernetes di origine
  - Cluster Kubernetes di destinazione
  - Cluster ONTAP associati

- **Account utente**: Quando si aggiunge un backend di storage ONTAP al centro di controllo Astra, applicare le credenziali utente con il ruolo "admin". Questo ruolo dispone di metodi di accesso `http` e. `ontapi` Abilitato sia sui cluster di origine che di destinazione ONTAP. Fare riferimento a. "Gestire gli account utente nella documentazione di ONTAP" per ulteriori informazioni.

  Astra Control Provisioner only: Se hai abilitato la funzionalità Astra Control Provisioner, non hai più bisogno di definire specificamente un ruolo "admin" per gestire i cluster in Astra Control Center, poiché queste credenziali non sono più necessarie all'interno di Astra Control Center.

"Implementare Astra Control Center" in un terzo dominio di errore o sito secondario per un disaster recovery perfetto.

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

Configurazione di Astra Trident/ONTAP

Astra Control Center richiede la configurazione di almeno un backend di storage che supporti la replica per i cluster di origine e di destinazione. Se i cluster di origine e di destinazione sono gli stessi, l'applicazione di destinazione deve utilizzare un backend di storage diverso da quello dell'applicazione di origine per ottenere la migliore resilienza.

La replica di Astra Control supporta le applicazioni che utilizzano una singola classe di storage. 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. Quando si aggiunge un PVC a un'applicazione replicata, assicurarsi che il nuovo PVC abbia la stessa classe di storage degli altri PVC nello spazio dei nomi.

Impostare una relazione di replica

L'impostazione di una relazione di replica comporta quanto segue:

- Scelta della frequenza con cui Astra Control deve acquisire uno snapshot dell'applicazione (che include le risorse Kubernetes dell'applicazione e le snapshot dei volumi per ciascun volume dell'applicazione)
- Scelta della pianificazione della replica (incluse le risorse Kubernetes e i dati dei volumi persistenti)
- Impostazione dell'ora in cui eseguire l'istantanea

Fasi

1. Dalla barra di navigazione a sinistra di Astra Control, selezionare **applicazioni**.
2. Selezionare la scheda **Data Protection** > **Replication**.
3. Selezionare **Configura policy di replica**. In alternativa, dalla casella protezione applicazione, selezionare l'opzione azioni e selezionare **Configura policy di replica**.
4. Inserire o selezionare le seguenti informazioni:
   - **Destination cluster** (cluster di destinazione): Inserire un cluster di destinazione (che può essere lo

stesso del cluster di origine).

- **Destination storage class** (Classe di storage di destinazione): Selezionare o immettere la classe di storage che utilizza la SVM in peering sul cluster ONTAP di destinazione. Come Best practice, la classe di storage di destinazione deve puntare a un backend di storage diverso da quello della classe di storage di origine.
- **Tipo di replica**: `Asynchronous` è attualmente l'unico tipo di replica disponibile.
- **Destination namespace** (spazio dei nomi di destinazione): Immettere spazi dei nomi di destinazione nuovi o esistenti per il cluster di destinazione.
- (Facoltativo) aggiungere spazi dei nomi aggiuntivi selezionando **Aggiungi spazio dei nomi** e scegliendo lo spazio dei nomi dall'elenco a discesa.
- **Replication frequency** (frequenza di replica): Consente di impostare la frequenza con cui Astra Control deve acquisire uno snapshot e replicarlo nella destinazione.
- **Offset**: Consente di impostare il numero di minuti dall'inizio dell'ora in cui si desidera che Astra Control prenda un'istantanea. È possibile utilizzare un offset in modo che non coincidano con altre operazioni pianificate.

Eseguire l'offset delle pianificazioni di backup e replica per evitare sovrapposizioni di pianificazione. Ad esempio, eseguire backup all'inizio dell'ora ogni ora e pianificare la replica per iniziare con un offset di 5 minuti e un intervallo di 10 minuti.

5. Selezionare **Avanti**, rivedere il riepilogo e selezionare **Salva**.

All'inizio, lo stato visualizza "app-mirror" prima che si verifichi la prima pianificazione.

Astra Control crea uno snapshot dell'applicazione utilizzato per la replica.

6. Per visualizzare lo stato dell'istantanea dell'applicazione, selezionare la scheda **applicazioni** > **istantanee**.

Il nome dello snapshot utilizza il formato di `replication-schedule-<string>`. Astra Control conserva l'ultimo snapshot utilizzato per la replica. Eventuali snapshot di replica meno recenti vengono eliminati dopo il completamento della replica.

Risultato

In questo modo si crea la relazione di replica.

Astra Control completa le seguenti azioni in seguito alla definizione della relazione:

- Crea uno spazio dei nomi sulla destinazione (se non esiste)
- Crea un PVC sullo spazio dei nomi di destinazione corrispondente ai PVC dell'applicazione di origine.
- Crea uno snapshot iniziale coerente con l'applicazione.
- Stabilisce la relazione di SnapMirror per i volumi persistenti utilizzando lo snapshot iniziale.

La pagina **Data Protection** mostra lo stato e lo stato della relazione di replica:
<Health status> | <Relationship life cycle state>

Ad esempio:
Normale | stabilito

Scopri di più sugli stati e sullo stato della replica alla fine di questo argomento.

Portare online un'applicazione replicata sul cluster di destinazione (failover)

Utilizzando Astra Control, è possibile eseguire il failover delle applicazioni replicate in un cluster di destinazione. Questa procedura interrompe la relazione di replica e porta l'applicazione online sul cluster di destinazione. Questa procedura non interrompe l'applicazione sul cluster di origine se era operativa.

Fasi

1. Dalla barra di navigazione a sinistra di Astra Control, selezionare **applicazioni**.
2. Selezionare la scheda **Data Protection** > **Replication**.
3. Dal menu Actions (azioni), selezionare **failover**.
4. Nella pagina failover, esaminare le informazioni e selezionare **failover**.

Risultato

Le seguenti azioni si verificano in seguito alla procedura di failover:

- L'applicazione di destinazione viene avviata in base all'ultimo snapshot replicato.
- Il cluster e l'applicazione di origine (se operativi) non vengono arrestati e continueranno a funzionare.
- Lo stato di replica cambia in "failover", quindi in "failover" una volta completato.
- La policy di protezione dell'applicazione di origine viene copiata nell'applicazione di destinazione in base alle pianificazioni presenti nell'applicazione di origine al momento del failover.
- Se nell'applicazione di origine sono attivati uno o più hook di esecuzione post-ripristino, tali hook di esecuzione vengono eseguiti per l'applicazione di destinazione.
- Astra Control mostra l'applicazione sia sul cluster di origine che di destinazione, nonché il relativo stato di salute.

Risincronizzare una replica con esito negativo

L'operazione di risincronizzazione ristabilisce la relazione di replica. È possibile scegliere l'origine della relazione per conservare i dati nel cluster di origine o di destinazione. Questa operazione ristabilisce le relazioni di SnapMirror per avviare la replica del volume nella direzione desiderata.

Il processo arresta l'applicazione sul nuovo cluster di destinazione prima di ristabilire la replica.

Durante il processo di risincronizzazione, lo stato del ciclo di vita viene visualizzato come "stabiling" (in corso).

Fasi

1. Dalla barra di navigazione a sinistra di Astra Control, selezionare **applicazioni**.
2. Selezionare la scheda **Data Protection** > **Replication**.
3. Dal menu Actions (azioni), selezionare **Resync**.
4. Nella pagina Resync, selezionare l'istanza dell'applicazione di origine o di destinazione contenente i dati che si desidera conservare.

Scegliere con attenzione l'origine di risincronizzazione, in quanto i dati sulla destinazione verranno sovrascritti.

5. Selezionare **Resync** per continuare.
6. Digitare "resync" per confermare.
7. Selezionare **Sì, risincronizzare** per terminare.

Risultato

- La pagina Replication (Replica) mostra "stabiling" (in corso) come stato della replica.
- Astra Control arresta l'applicazione sul nuovo cluster di destinazione.
- Astra Control ristabilisce la replica del volume persistente nella direzione selezionata utilizzando la risincronizzazione di SnapMirror.
- La pagina Replication mostra la relazione aggiornata.

Replica inversa delle applicazioni

Si tratta dell'operazione pianificata per spostare l'applicazione nel back-end dello storage di destinazione continuando a replicare nel back-end dello storage di origine. Astra Control arresta l'applicazione di origine e replica i dati nella destinazione prima di eseguire il failover nell'applicazione di destinazione.

In questa situazione, si sta sostituendo l'origine e la destinazione.

Fasi

1. Dalla barra di navigazione a sinistra di Astra Control, selezionare **applicazioni**.
2. Selezionare la scheda **Data Protection** > **Replication**.
3. Dal menu Actions (azioni), selezionare **Reverse Replication** (replica inversa).
4. Nella pagina Replica inversa, esaminare le informazioni e selezionare **Replica inversa** per continuare.

Risultato

Le seguenti azioni si verificano in seguito alla replica inversa:

- Viene acquisita un'istantanea delle risorse Kubernetes dell'applicazione di origine.
- I pod dell'applicazione di origine vengono interrotti correttamente eliminando le risorse Kubernetes dell'applicazione (lasciando PVC e PVS in posizione).
- Una volta spenti i pod, vengono acquisite e replicate le istantanee dei volumi dell'applicazione.
- Le relazioni di SnapMirror vengono interrotte, rendendo i volumi di destinazione pronti per la lettura/scrittura.
- Le risorse Kubernetes dell'applicazione vengono ripristinate dallo snapshot pre-shutdown, utilizzando i dati del volume replicati dopo l'arresto dell'applicazione di origine.
- La replica viene ristabilita in senso inverso.

Eseguire il failback delle applicazioni nel cluster di origine originale

Utilizzando Astra Control, è possibile ottenere il "failback" dopo un'operazione di failover utilizzando la seguente sequenza di operazioni. In questo flusso di lavoro per ripristinare la direzione di replica originale, Astra Control replica (risincronizza) le modifiche dell'applicazione nell'applicazione di origine prima di invertire la direzione di replica.

Questo processo inizia da una relazione che ha completato un failover verso una destinazione e prevede i seguenti passaggi:

- Iniziare con uno stato di failover.
- Risincronizzare la relazione.
- Invertire la replica.

Fasi

1. Dalla barra di navigazione a sinistra di Astra Control, selezionare **applicazioni**.
2. Selezionare la scheda **Data Protection** > **Replication**.
3. Dal menu Actions (azioni), selezionare **Resync**.
4. Per un'operazione di fail back, scegliere l'applicazione failed over come origine dell'operazione di risync (mantenendo i dati scritti dopo il failover).
5. Digitare "resync" per confermare.
6. Selezionare **Sì, risincronizzare** per terminare.
7. Al termine della risincronizzazione, nel menu azioni della scheda protezione dati > Replica, selezionare **Replica inversa**.
8. Nella pagina Replica inversa, esaminare le informazioni e selezionare **Replica inversa**.

Risultato

Questo combina i risultati delle operazioni di "risincronizzazione" e "reverse relationship" per portare l'applicazione online sul cluster di origine con la replica ripresa nel cluster di destinazione originale.

Eliminare una relazione di replica dell'applicazione

L'eliminazione della relazione comporta due applicazioni separate senza alcuna relazione tra di esse.

Fasi

1. Dalla barra di navigazione a sinistra di Astra Control, selezionare **applicazioni**.
2. Selezionare la scheda **Data Protection** > **Replication**.
3. Nella casella protezione applicazione o nel diagramma delle relazioni, selezionare **Elimina relazione di replica**.

Risultato

Le seguenti azioni si verificano in seguito all'eliminazione di una relazione di replica:

- Se la relazione viene stabilita ma l'applicazione non è ancora stata messa in linea sul cluster di destinazione (failover), Astra Control conserva i PVC creati durante l'inizializzazione, lascia un'applicazione gestita "vuota" sul cluster di destinazione e conserva l'applicazione di destinazione per conservare eventuali backup creati.
- Se l'applicazione è stata portata online sul cluster di destinazione (failover), Astra Control conserva PVC e applicazioni di destinazione. Le applicazioni di origine e di destinazione sono ora considerate come applicazioni indipendenti. Le pianificazioni di backup rimangono su entrambe le applicazioni ma non sono associate l'una all'altra.

stato di salute della relazione di replica e stati del ciclo di vita della relazione

Astra Control visualizza lo stato della relazione e gli stati del ciclo di vita della relazione di replica.

Stati di integrità delle relazioni di replica

I seguenti stati indicano lo stato della relazione di replica:

- **Normale**: La relazione sta stabilendo o è stata stabilita e lo snapshot più recente è stato trasferito correttamente.
- **Attenzione**: La relazione sta fallendo o ha avuto un failover (e quindi non protegge più l'applicazione di origine).
- **Critico**
  - La relazione sta stabilendo o fallendo e l'ultimo tentativo di riconciliazione non è riuscito.
  - La relazione viene stabilita e l'ultimo tentativo di riconciliare l'aggiunta di un nuovo PVC sta fallendo.
  - La relazione viene stabilita (in modo da replicare uno snapshot di successo ed è possibile eseguire il failover), ma lo snapshot più recente non è riuscito o non è riuscito a replicarsi.

stati del ciclo di vita della replica

I seguenti stati riflettono le diverse fasi del ciclo di vita della replica:

- **Definizione**: È in corso la creazione di una nuova relazione di replica. Astra Control crea uno spazio dei nomi, se necessario, crea dichiarazioni di volumi persistenti (PVC) su nuovi volumi nel cluster di destinazione e crea relazioni SnapMirror. Questo stato può anche indicare che la replica sta eseguendo una risyncing o un'inversione della replica.
- **Stabilito**: Esiste una relazione di replica. Astra Control verifica periodicamente la disponibilità dei PVC, verifica la relazione di replica, crea periodicamente snapshot dell'applicazione e identifica eventuali nuovi PVC di origine nell'applicazione. In tal caso, Astra Control crea le risorse per includerle nella replica.
- **Failover**: Astra Control interrompe le relazioni di SnapMirror e ripristina le risorse Kubernetes dell'applicazione dall'ultimo snapshot dell'applicazione replicato con successo.
- **Failed over**: Astra Control interrompe la replica dal cluster di origine, utilizza lo snapshot dell'applicazione replicato più recente (riuscito) sulla destinazione e ripristina le risorse Kubernetes.
- **Risyncing**: Astra Control risincronizza i nuovi dati sull'origine resync alla destinazione resync utilizzando la risync di SnapMirror. Questa operazione potrebbe sovrascrivere alcuni dati sulla destinazione in base alla direzione della sincronizzazione. Astra Control interrompe l'esecuzione dell'applicazione sullo spazio dei nomi di destinazione e rimuove l'applicazione Kubernetes. Durante il processo di risyncing, lo stato viene visualizzato come "stabiling" (in corso).
- **Inversione**: È l'operazione pianificata per spostare l'applicazione nel cluster di destinazione continuando a replicare nel cluster di origine. Astra Control arresta l'applicazione sul cluster di origine, replica i dati nella destinazione prima di eseguire il failover dell'applicazione nel cluster di destinazione. Durante la replica inversa, lo stato viene visualizzato come "stabiling" (in corso).
- **Eliminazione**:
  - Se la relazione di replica è stata stabilita ma non è stato ancora eseguito il failover, Astra Control rimuove i PVC creati durante la replica ed elimina l'applicazione gestita di destinazione.
  - Se la replica ha già avuto esito negativo, Astra Control conserva i PVC e l'applicazione di destinazione.

Clonare e migrare le applicazioni

È possibile clonare un'applicazione esistente per creare un'applicazione duplicata sullo stesso cluster Kubernetes o su un altro cluster. Quando Astra Control clona un'applicazione, crea un clone della configurazione dell'applicazione e dello storage

persistente.

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 di Astra Control Center o. "API di controllo Astra" per clonare e migrare le applicazioni.

Prima di iniziare

- **Check destination Volumes** (Controlla volumi di destinazione): Se si esegue la clonazione in una classe di storage diversa, assicurarsi che la classe di storage utilizzi la stessa modalità di accesso al volume persistente (ad esempio ReadWriteMany). L'operazione di clonazione non riesce se la modalità di accesso al volume persistente di destinazione è diversa. Ad esempio, se il volume persistente di origine utilizza la modalità di accesso RWX, selezionare una classe di storage di destinazione che non è in grado di fornire RWX, come Azure Managed Disks, AWS EBS, Google Persistent Disk o. `ontap-san`, causerà l'errore dell'operazione di clonazione. Per ulteriori informazioni sulle modalità di accesso al volume persistente, fare riferimento a. "Kubernetes" documentazione.
- Per clonare le applicazioni in un cluster diverso, è necessario assicurarsi che le istanze cloud che contengono i cluster di origine e di destinazione (se non sono uguali) abbiano un bucket predefinito. Sarà necessario assegnare un bucket predefinito per ogni istanza del cloud.
- 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.

> Durante la clonazione delle applicazioni in ambienti OpenShift, Astra Control Center deve consentire a OpenShift di montare volumi e modificare la proprietà dei file. Per questo motivo, è necessario configurare un criterio di esportazione dei volumi ONTAP per consentire queste operazioni. Puoi farlo con i seguenti comandi:
>
> 1. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -superuser sys`
> 2. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -anon 65534`

Limitazioni dei cloni

- **Classi di storage esplicite**: Se si implementa un'applicazione con una classe di storage esplicitamente impostata e si deve clonare l'applicazione, il cluster di destinazione deve avere la classe di storage specificata in origine. La clonazione di un'applicazione con una classe di storage esplicitamente impostata su un cluster che non ha la stessa classe di storage non avrà esito positivo.
- **Applicazioni supportate da ontap-nas a economia**: Non è possibile utilizzare le operazioni di clonazione se la classe di storage dell'applicazione è supportata da `ontap-nas-economy` driver. Tuttavia, è possibile "abilita backup e ripristino per le operazioni economiche a ontap-nas".
- **Cloni e vincoli dell'utente**: Qualsiasi utente membro con vincoli dello spazio dei nomi in base al nome/ID dello spazio dei nomi o alle etichette dello spazio dei nomi può clonare o ripristinare un'applicazione in un nuovo spazio dei nomi sullo stesso cluster o in qualsiasi altro cluster dell'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 l'account utente membro e aggiornare i vincoli di ruolo affinché l'utente interessato conceda l'accesso al nuovo spazio dei nomi.
- **I cloni utilizzano bucket predefiniti**: Durante il backup o il ripristino di un'applicazione, è possibile specificare un ID bucket. Un'operazione di cloni dell'applicazione, tuttavia, utilizza sempre il bucket predefinito definito. Non esiste alcuna opzione per modificare i bucket per un clone. Se si desidera

controllare quale bucket viene utilizzato, è possibile farlo "modificare l'impostazione predefinita del bucket" oppure fare una "backup" seguito da un "ripristinare" separatamente.

- **Con Jenkins ci**: Se si clonano istanze distribuite dall'operatore di Jenkins ci, è necessario ripristinare manualmente i dati persistenti. Si tratta di un limite del modello di implementazione dell'applicazione.
- **Con i bucket S3**: 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.
- **Con una versione specifica di PostgreSQL**: I cloni delle applicazioni all'interno dello stesso cluster si guastano costantemente con il grafico BitNami PostgreSQL 11.5.0. Per clonare correttamente, utilizzare una versione precedente o successiva del grafico.

Considerazioni su OpenShift

- **Versioni di Clusters e OpenShift**: Se clonate un'applicazione tra cluster, i cluster di origine e di destinazione devono essere la 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.
- **Progetti e UID**: 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. Selezionare **applicazioni**.
2. Effettuare una delle seguenti operazioni:
   - Selezionare il menu Options (Opzioni) nella colonna **Actions** (azioni) per l'applicazione desiderata.
   - Selezionare il nome dell'applicazione desiderata e l'elenco a discesa Status (Stato) in alto a destra nella pagina.
3. Selezionare **Clone**.
4. Specificare i dettagli per il clone:
   - Immettere un nome.
   - Scegliere un cluster di destinazione per il clone.
   - Immettere gli spazi dei nomi di destinazione per il clone. Ogni namespace di origine associato all'applicazione viene mappato allo spazio dei nomi di destinazione definito dall'utente.

     Astra Control crea nuovi spazi dei nomi di destinazione come parte dell'operazione di clone. Gli spazi dei nomi di destinazione specificati non devono essere già presenti nel cluster di destinazione.

   - Selezionare **Avanti**.
   - Scegliere di mantenere la classe di storage originale associata all'applicazione o di selezionare una classe di storage diversa.

Puoi migrare la classe di storage di un'app a una classe di storage di un cloud provider nativo o a un'altra classe di storage supportata, migrare un'app da una classe di storage supportata da `ontap-nas-economy` a una classe di storage supportata da `ontap-nas` sullo stesso cluster oppure copiare l'applicazione in un altro cluster con una classe di storage supportata da `ontap-nas-economy` driver.

Se si seleziona una classe di storage diversa e questa classe di storage non esiste al momento del ripristino, viene restituito un errore.

5. Selezionare **Avanti**.
6. Esaminare le informazioni relative al clone e selezionare **Clone**.

Risultato

Astra Control clona l'applicazione in base alle informazioni fornite. L'operazione di clonazione viene eseguita correttamente quando il nuovo clone dell'applicazione è attivo `Healthy` nella pagina **applicazioni**.

Dopo che un'operazione di clonazione o ripristino crea un nuovo spazio dei nomi, l'amministratore/proprietario dell'account può modificare l'account utente membro e aggiornare i vincoli di ruolo affinché l'utente interessato conceda l'accesso al nuovo spazio dei nomi.

Dopo un'operazione di protezione dei dati (clone, backup o 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 gli hook di esecuzione delle applicazioni

Un gancio di esecuzione è un'azione personalizzata che è possibile configurare per l'esecuzione in combinazione con un'operazione di protezione dei dati di un'applicazione gestita. Ad esempio, se si dispone di un'applicazione di database, è possibile utilizzare un gancio di esecuzione per mettere in pausa tutte le transazioni del database prima di uno snapshot e riprendere le transazioni al termine dello snapshot. Ciò garantisce snapshot coerenti con l'applicazione.

Tipi di hook di esecuzione

Astra Control Center supporta i seguenti tipi di hook di esecuzione, in base al momento in cui possono essere eseguiti:

- Pre-snapshot
- Post-snapshot
- Pre-backup
- Post-backup
- Post-ripristino
- Post-failover

Esecuzione dei filtri hook

Quando si aggiunge o si modifica un gancio di esecuzione a un'applicazione, è possibile aggiungere filtri a un gancio di esecuzione per gestire i contenitori corrispondenti. I filtri sono utili per le applicazioni che utilizzano la stessa immagine container su tutti i container, ma possono utilizzare ogni immagine per uno scopo diverso (ad esempio Elasticsearch). I filtri consentono di creare scenari in cui gli hook di esecuzione vengono eseguiti su alcuni container identici, ma non necessariamente su tutti. Se si creano più filtri per un singolo gancio di esecuzione, questi vengono combinati con un operatore AND logico. È possibile avere fino a 10 filtri attivi per gancio di esecuzione.

Ogni filtro aggiunto a un gancio di esecuzione utilizza un'espressione regolare per far corrispondere i contenitori nel cluster. Quando un gancio corrisponde a un container, il gancio esegue lo script associato su quel container. Le espressioni regolari per i filtri utilizzano la sintassi RE2 (espressione regolare), che non supporta la creazione di un filtro che esclude i contenitori dall'elenco di corrispondenze. Per informazioni sulla sintassi supportata da Astra Control per le espressioni regolari nei filtri hook di esecuzione, vedere "Supporto della sintassi RE2 (Regular Expression 2)".

> Se si aggiunge un filtro dello spazio dei nomi a un gancio di esecuzione che viene eseguito dopo un'operazione di ripristino o clonazione e l'origine e la destinazione del ripristino o del clone si trovano in spazi dei nomi diversi, il filtro dello spazio dei nomi viene applicato solo allo spazio dei nomi di destinazione.

Note importanti sugli hook di esecuzione personalizzati

Quando si pianificano gli hook di esecuzione per le applicazioni, considerare quanto segue.

> Poiché gli hook di esecuzione spesso riducono o disattivano completamente le funzionalità dell'applicazione con cui vengono eseguiti, si consiglia di ridurre al minimo il tempo necessario per l'esecuzione degli hook di esecuzione personalizzati.
> Se si avvia un'operazione di backup o snapshot con gli hook di esecuzione associati, ma poi si annulla, gli hook possono ancora essere eseguiti se l'operazione di backup o snapshot è già iniziata. Ciò significa che la logica utilizzata in un gancio di esecuzione post-backup non può presumere che il backup sia stato completato.

- La funzionalità hook di esecuzione è disabilitata per impostazione predefinita per le nuove implementazioni di Astra Control.
  - È necessario attivare la funzione di hook di esecuzione prima di poter utilizzare i hook di esecuzione.
  - Gli utenti proprietari o amministratori possono attivare o disattivare la funzionalità di hook di esecuzione per tutti gli utenti definiti nell'account Astra Control corrente. Fare riferimento a. Attivare la funzione ganci di esecuzione e. Disattivare la funzione ganci di esecuzione per istruzioni.
  - Lo stato di abilitazione delle funzioni viene mantenuto durante gli aggiornamenti di Astra Control.
- Un gancio di esecuzione deve utilizzare uno script per eseguire le azioni. Molti hook di esecuzione possono fare riferimento allo stesso script.
- Astra Control richiede che gli script utilizzati dagli hook di esecuzione siano scritti nel formato degli script shell eseguibili.
- La dimensione dello script è limitata a 96 KB.
- Astra Control utilizza le impostazioni degli uncino di esecuzione e qualsiasi criterio corrispondente per determinare quali hook sono applicabili a un'operazione di snapshot, backup o ripristino.
- Tutti i guasti degli uncini di esecuzione sono guasti di tipo soft; altri hook e l'operazione di protezione dei dati vengono ancora tentati anche in caso di interruzione di un hook. Tuttavia, quando un gancio non

funziona, viene registrato un evento di avviso nel registro eventi della pagina **attività**.

- Per creare, modificare o eliminare gli hook di esecuzione, è necessario essere un utente con autorizzazioni Owner, Admin o Member.
- Se l'esecuzione di un gancio di esecuzione richiede più di 25 minuti, l'hook non riesce, creando una voce del registro eventi con un codice di ritorno "N/A". Qualsiasi snapshot interessata verrà contrassegnata come non riuscita e una voce del registro eventi risultante annoterà il timeout.
- Per le operazioni di protezione dei dati ad hoc, tutti gli eventi hook vengono generati e salvati nel registro eventi della pagina **Activity**. Tuttavia, per le operazioni di protezione dei dati pianificate, nel registro eventi vengono registrati solo gli eventi di errore hook (gli eventi generati dalle operazioni di protezione dei dati pianificate vengono ancora registrati).
- Se Astra Control Center esegue il failover di un'applicazione di origine replicata nell'applicazione di destinazione, tutti gli hook di esecuzione post-failover abilitati per l'applicazione di origine vengono eseguiti per l'applicazione di destinazione al termine del failover.

> Se sono stati eseguiti hook dopo il ripristino con Astra Control Center 23,04 e l'Astra Control Center è stato aggiornato alla versione 23,07 o successiva, i hook di esecuzione post-ripristino non verranno più eseguiti dopo una replica di failover. Devi creare nuovi hook di esecuzione post-failover per le tue applicazioni. In alternativa, è possibile modificare il tipo di operazione degli hook post-ripristino esistenti destinati ai failover da "post-ripristino" a "post-failover".

Ordine di esecuzione

Quando viene eseguita un'operazione di protezione dei dati, gli eventi hook di esecuzione hanno luogo nel seguente ordine:

1. Gli eventuali hook di esecuzione pre-operation personalizzati applicabili vengono eseguiti sui container appropriati. È possibile creare ed eseguire tutti gli hook pre-operation personalizzati necessari, ma l'ordine di esecuzione di questi hook prima dell'operazione non è garantito né configurabile.
2. Viene eseguita l'operazione di protezione dei dati.
3. Gli eventuali hook di esecuzione post-operation personalizzati applicabili vengono eseguiti sui container appropriati. È possibile creare ed eseguire tutti gli hook post-operation personalizzati necessari, ma l'ordine di esecuzione di questi hook dopo l'operazione non è garantito né configurabile.

Se si creano più hook di esecuzione dello stesso tipo (ad esempio, pre-snapshot), l'ordine di esecuzione di tali hook non è garantito. Tuttavia, è garantito l'ordine di esecuzione di ganci di tipi diversi. Ad esempio, l'ordine di esecuzione di una configurazione con tutti i diversi tipi di hook è simile al seguente:

1. Hook pre-backup eseguiti
2. Hook pre-snapshot eseguiti
3. Esecuzione di hook post-snapshot
4. Hook post-backup eseguiti
5. Esecuzione degli hook di post-ripristino

È possibile vedere un esempio di questa configurazione nello scenario numero 2 dalla tabella nella Determinare se verrà eseguito un gancio.

Prima di abilitarli in un ambiente di produzione, è necessario verificare sempre gli script hook di esecuzione. È possibile utilizzare il comando 'kubectl exec' per testare comodamente gli script. Dopo aver attivato gli hook di esecuzione in un ambiente di produzione, testare le snapshot e i backup risultanti per assicurarsi che siano coerenti. Per eseguire questa operazione, clonare l'applicazione in uno spazio dei nomi temporaneo, ripristinare lo snapshot o il backup e quindi testare l'applicazione.

Determinare se verrà eseguito un gancio

Utilizza la seguente tabella per determinare se verrà eseguito un gancio di esecuzione personalizzato per l'applicazione.

Si noti che tutte le operazioni di alto livello delle applicazioni consistono nell'eseguire una delle operazioni di base di snapshot, backup o ripristino. A seconda dello scenario, un'operazione di cloni può consistere in varie combinazioni di queste operazioni, quindi gli hook di esecuzione eseguiti da un'operazione di cloni variano.

Le operazioni di ripristino in-place richiedono un'istantanea o un backup esistente, in modo che queste operazioni non eseguano snapshot o hook di backup.

Se si avvia e poi si annulla un backup che include uno snapshot e sono associati degli hook di esecuzione, alcuni hook potrebbero essere eseguiti e altri no. Ciò significa che un gancio di esecuzione post-backup non può presumere che il backup sia stato completato. Tenere presente i seguenti punti per i backup annullati con gli hook di esecuzione associati:

- Gli hook pre-backup e post-backup sono sempre in esecuzione.
- Se il backup include un nuovo snapshot e lo snapshot è stato avviato, vengono eseguiti gli hook pre-snapshot e post-snapshot.
- Se il backup viene annullato prima dell'avvio dello snapshot, gli hook pre-snapshot e post-snapshot non vengono eseguiti.

Scenario	Operazione	Snapshot esistente	Backup esistente	Namespace	Cluster	Esecuzione di Snapshot Hooks	Esecuzione dei ganci di backup	Esecuzione degli hook di ripristino	Esecuzione degli hook di failover
1	Clonare	N	N	Novità	Stesso	Y	N	Y	N
2	Clonare	N	N	Novità	Diverso	Y	Y	Y	N
3	Clonare o ripristinare	Y	N	Novità	Stesso	N	N	Y	N
4	Clonare o ripristinare	N	Y	Novità	Stesso	N	N	Y	N
5	Clonare o ripristinare	Y	N	Novità	Diverso	N	N	Y	N
6	Clonare o ripristinare	N	Y	Novità	Diverso	N	N	Y	N

Scenario	Operazione	Snapshot esistente	Backup esistente	Namespace	Cluster	Esecuzione di Snapshot Hooks	Esecuzione dei ganci di backup	Esecuzione degli hook di ripristino	Esecuzione degli hook di failover
7	Ripristinare	Y	N	Esistente	Stesso	N	N	Y	N
8	Ripristinare	N	Y	Esistente	Stesso	N	N	Y	N
9	Snapshot	N/A.	N/A.	N/A.	N/A.	Y	N/A.	N/A.	N
10	Backup	N	N/A.	N/A.	N/A.	Y	Y	N/A.	N
11	Backup	Y	N/A.	N/A.	N/A.	N	N	N/A.	N
12	Failover	Y	N/A.	Creato dalla replica	Diverso	N	N	N	Y
13	Failover	Y	N/A.	Creato dalla replica	Stesso	N	N	N	Y

Esempi di gancio di esecuzione

Visitare il "Progetto NetApp Verda GitHub" Per scaricare gli hook di esecuzione per le applicazioni più diffuse come Apache Cassandra ed Elasticsearch. Puoi anche vedere esempi e trovare idee per strutturare i tuoi hook di esecuzione personalizzati.

Attivare la funzione ganci di esecuzione

Se si è un utente Proprietario o Amministratore, è possibile attivare la funzione ganci di esecuzione. Quando si attiva la funzionalità, tutti gli utenti definiti in questo account Astra Control possono utilizzare i ganci di esecuzione e visualizzare i ganci di esecuzione e gli script hook esistenti.

Fasi

1. Accedere a **applicazioni** e selezionare il nome di un'applicazione gestita.
2. Selezionare la scheda **Execution Hooks**.
3. Selezionare **Abilita ganci di esecuzione**.

   Viene visualizzata la scheda **account** > **Impostazioni funzioni**.

4. Nel riquadro **ganci di esecuzione**, selezionare il menu delle impostazioni.
5. Selezionare **Abilita**.
6. Prendere nota dell'avviso di protezione visualizzato.
7. Selezionare **Sì, abilita i ganci di esecuzione**.

Disattivare la funzione ganci di esecuzione

Se si è un utente Proprietario o Amministratore, è possibile disattivare la funzionalità Hook di esecuzione per tutti gli utenti definiti in questo account Astra Control. È necessario eliminare tutti i ganci di esecuzione esistenti prima di disattivare la funzione ganci di esecuzione. Fare riferimento a. Eliminare un gancio di esecuzione per

istruzioni sull'eliminazione di un gancio di esecuzione esistente.

Fasi

1. Andare su **account**, quindi selezionare la scheda **Impostazioni funzione**.
2. Selezionare la scheda **Execution Hooks**.
3. Nel riquadro **ganci di esecuzione**, selezionare il menu delle impostazioni.
4. Selezionare **Disable** (Disattiva).
5. Prendere nota dell'avviso visualizzato.
6. Tipo `disable` per confermare che si desidera disattivare la funzione per tutti gli utenti.
7. Selezionare **Sì, disabilita**.

Visualizzare gli hook di esecuzione esistenti

È possibile visualizzare gli hook di esecuzione personalizzati esistenti per un'applicazione.

Fasi

1. Accedere a **applicazioni** e selezionare il nome di un'applicazione gestita.
2. Selezionare la scheda **Execution Hooks**.

   È possibile visualizzare tutti gli hook di esecuzione attivati o disattivati nell'elenco risultante. È possibile visualizzare lo stato di un gancio, il numero di contenitori corrispondenti, il tempo di creazione e il momento in cui viene eseguito (pre- o post-operazione). È possibile selezionare + accanto al nome dell'hook per espandere l'elenco dei container su cui verrà eseguito. Per visualizzare i registri degli eventi relativi agli hook di esecuzione per questa applicazione, accedere alla scheda **attività**.

Visualizzare gli script esistenti

È possibile visualizzare gli script caricati. In questa pagina puoi anche vedere quali script sono in uso e quali hook li stanno utilizzando.

Fasi

1. Vai a **account**.
2. Selezionare la scheda **script**.

   In questa pagina è possibile visualizzare un elenco degli script caricati. La colonna **Used by** mostra gli hook di esecuzione che utilizzano ogni script.

Aggiungere uno script

Ogni gancio di esecuzione deve utilizzare uno script per eseguire le azioni. È possibile aggiungere uno o più script a cui possono fare riferimento gli hook di esecuzione. Molti hook di esecuzione possono fare riferimento allo stesso script; ciò consente di aggiornare molti hook di esecuzione modificando solo uno script.

Fasi

1. Verificare che la funzione ganci di esecuzione sia attivato.
2. Vai a **account**.
3. Selezionare la scheda **script**.

4. Selezionare **Aggiungi**.
5. Effettuare una delle seguenti operazioni:
   - Caricare uno script personalizzato.
     i. Selezionare l'opzione **carica file**.
     ii. Selezionare un file e caricarlo.
     iii. Assegnare allo script un nome univoco.
     iv. (Facoltativo) inserire eventuali note che altri amministratori dovrebbero conoscere sullo script.
     v. Selezionare **Salva script**.
   - Incollare uno script personalizzato dagli Appunti.
     i. Selezionare l'opzione **Incolla o tipo**.
     ii. Selezionare il campo di testo e incollare il testo dello script nel campo.
     iii. Assegnare allo script un nome univoco.
     iv. (Facoltativo) inserire eventuali note che altri amministratori dovrebbero conoscere sullo script.
6. Selezionare **Salva script**.

Risultato

Il nuovo script viene visualizzato nell'elenco della scheda **script**.

Eliminare uno script

È possibile rimuovere uno script dal sistema se non è più necessario e non viene utilizzato da alcun hook di esecuzione.

Fasi

1. Vai a **account**.
2. Selezionare la scheda **script**.
3. Scegliere uno script da rimuovere e selezionare il menu nella colonna **azioni**.
4. Selezionare **Delete** (Elimina).

> Se lo script è associato a uno o più hook di esecuzione, l'azione **Delete** non è disponibile. Per eliminare lo script, modificare prima gli hook di esecuzione associati e associarli a uno script diverso.

Creare un gancio di esecuzione personalizzato

È possibile creare un gancio di esecuzione personalizzato per un'applicazione e aggiungerlo ad Astra Control. Fare riferimento a. Esempi di gancio di esecuzione per esempi di gancio. Per creare gli hook di esecuzione, è necessario disporre delle autorizzazioni Owner (Proprietario), Admin (Amministratore) o Member (membro).

> Quando si crea uno script shell personalizzato da utilizzare come uncino di esecuzione, ricordarsi di specificare la shell appropriata all'inizio del file, a meno che non si stiano eseguendo comandi specifici o fornendo il percorso completo di un eseguibile.

Fasi

1. Verificare che la funzione ganci di esecuzione sia attivato.

2. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione gestita.
3. Selezionare la scheda **Execution Hooks**.
4. Selezionare **Aggiungi**.
5. Nell'area **Dettagli gancio**:
   a. Determinare quando il gancio deve funzionare selezionando un tipo di operazione dal menu a discesa **operazione**.
   b. Immettere un nome univoco per l'hook.
   c. (Facoltativo) inserire gli argomenti da passare al gancio durante l'esecuzione, premendo il tasto Invio dopo ogni argomento inserito per registrarne ciascuno.
6. (Facoltativo) nell'area **Dettagli filtro gancio**, è possibile aggiungere filtri per controllare i contenitori su cui viene eseguito l'gancio di esecuzione:
   a. Selezionare **Aggiungi filtro**.
   b. Nella colonna **tipo filtro gancio**, scegliere un attributo sul quale filtrare dal menu a discesa.
   c. Nella colonna **Regex**, immettere un'espressione regolare da utilizzare come filtro. Astra Control utilizza "Sintassi regex espressione regolare 2 (RE2)".

      Se si filtra sul nome esatto di un attributo (ad esempio il nome di un pod) senza altro testo nel campo di espressione regolare, viene eseguita una corrispondenza di sottostringa. Per associare un nome esatto e solo il nome, utilizzare la sintassi di corrispondenza stringa esatta (ad esempio, `^exact_podname$`).

   d. Per aggiungere altri filtri, selezionare **Aggiungi filtro**.

      I filtri multipli per un gancio di esecuzione sono combinati con un operatore and logico. È possibile avere fino a 10 filtri attivi per gancio di esecuzione.

7. Al termine, selezionare **Avanti**.
8. Nell'area **script**, eseguire una delle seguenti operazioni:
   - Aggiungere un nuovo script.
     i. Selezionare **Aggiungi**.
     ii. Effettuare una delle seguenti operazioni:
       - Caricare uno script personalizzato.
         I. Selezionare l'opzione **carica file**.
         II. Selezionare un file e caricarlo.
         III. Assegnare allo script un nome univoco.
         IV. (Facoltativo) inserire eventuali note che altri amministratori dovrebbero conoscere sullo script.
         V. Selezionare **Salva script**.
       - Incollare uno script personalizzato dagli Appunti.
         I. Selezionare l'opzione **Incolla o tipo**.
         II. Selezionare il campo di testo e incollare il testo dello script nel campo.
         III. Assegnare allo script un nome univoco.

IV. (Facoltativo) inserire eventuali note che altri amministratori dovrebbero conoscere sullo script.

- Selezionare uno script esistente dall'elenco.

  In questo modo, il gancio di esecuzione deve utilizzare questo script.

9. Selezionare **Avanti**.
10. Esaminare la configurazione degli uncino di esecuzione.
11. Selezionare **Aggiungi**.

Controllare lo stato di un gancio di esecuzione

Al termine dell'esecuzione di un'operazione di snapshot, backup o ripristino, è possibile controllare lo stato degli hook di esecuzione eseguiti come parte dell'operazione. È possibile utilizzare queste informazioni di stato per determinare se si desidera mantenere l'esecuzione agganciata, modificarla o eliminarla.

Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione gestita.
2. Selezionare la scheda **Data Protection**.
3. Selezionare **Snapshot** per visualizzare le snapshot in esecuzione o **Backup** per visualizzare i backup in esecuzione.

   Lo stato **Hook** mostra lo stato dell'esecuzione dell'hook al termine dell'operazione. Per ulteriori informazioni, passare il mouse sullo stato. Ad esempio, se si verificano errori di uncino di esecuzione durante uno snapshot, passando il mouse sullo stato di uncino per tale snapshot si ottiene un elenco di uncini di esecuzione non riusciti. Per visualizzare i motivi di ciascun guasto, consultare la pagina **Activity** (attività) nell'area di navigazione a sinistra.

Visualizzare l'utilizzo dello script

È possibile vedere quali hook di esecuzione utilizzano uno script specifico nell'interfaccia utente Web di Astra Control.

Fasi

1. Selezionare **account**.
2. Selezionare la scheda **script**.

   La colonna **Used by** nell'elenco degli script contiene i dettagli su quali hook utilizzano ciascuno script dell'elenco.

3. Selezionare le informazioni nella colonna **utilizzato da** per lo script desiderato.

   Viene visualizzato un elenco più dettagliato con i nomi degli hook che utilizzano lo script e il tipo di operazione con cui sono configurati per l'esecuzione.

Modificare un gancio di esecuzione

È possibile modificare un gancio di esecuzione se si desidera modificarne gli attributi, i filtri o lo script utilizzato. Per modificare gli hook di esecuzione, è necessario disporre delle autorizzazioni Owner, Admin o Member.

Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione gestita.
2. Selezionare la scheda **Execution Hooks**.
3. Selezionare il menu Options (Opzioni) nella colonna **Actions** (azioni) per un gancio che si desidera modificare.
4. Selezionare **Modifica**.
5. Apportare le modifiche necessarie, selezionando **Avanti** dopo aver completato ciascuna sezione.
6. Selezionare **Salva**.

Disattiva un gancio di esecuzione

È possibile disattivare un gancio di esecuzione se si desidera impedirne temporaneamente l'esecuzione prima o dopo un'istantanea di un'applicazione. Per disattivare gli hook di esecuzione, è necessario disporre delle autorizzazioni Owner, Admin o Member.

Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione gestita.
2. Selezionare la scheda **Execution Hooks**.
3. Selezionare il menu Options (Opzioni) nella colonna **Actions** (azioni) per un gancio che si desidera disattivare.
4. Selezionare **Disable** (Disattiva).

Eliminare un gancio di esecuzione

È possibile rimuovere completamente un gancio di esecuzione se non è più necessario. Per eliminare gli hook di esecuzione, è necessario disporre delle autorizzazioni Owner, Admin o Member.

Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione gestita.
2. Selezionare la scheda **Execution Hooks**.
3. Selezionare il menu Options (Opzioni) nella colonna **Actions** (azioni) per il gancio che si desidera eliminare.
4. Selezionare **Delete** (Elimina).
5. Nella finestra di dialogo visualizzata, digitare "DELETE" per confermare.
6. Selezionare **Sì, elimina gancio di esecuzione**.

Per ulteriori informazioni

- "Progetto NetApp Verda GitHub"

Proteggi Astra Control Center con Astra Control Center

Per garantire una maggiore resilienza contro errori fatali nel cluster Kubernetes in cui è in esecuzione Astra Control Center, proteggere l'applicazione Astra Control Center stessa. Puoi eseguire il backup e il ripristino di Astra Control Center utilizzando un'istanza secondaria di Astra Control Center o utilizzare la replica Astra se lo storage sottostante utilizza ONTAP.

In questi scenari, una seconda istanza di Astra Control Center viene implementata e configurata in un dominio di errore diverso e viene eseguita in un secondo cluster Kubernetes diverso rispetto all'istanza primaria Astra Control Center. La seconda istanza di Astra Control viene utilizzata per eseguire il backup e ripristinare potenzialmente l'istanza primaria di Astra Control Center. Un'istanza di Astra Control Center, ripristinata o replicata, continuerà a fornire la gestione dei dati delle applicazioni per le applicazioni cluster e a ripristinare l'accessibilità ai backup e alle snapshot di tali applicazioni.

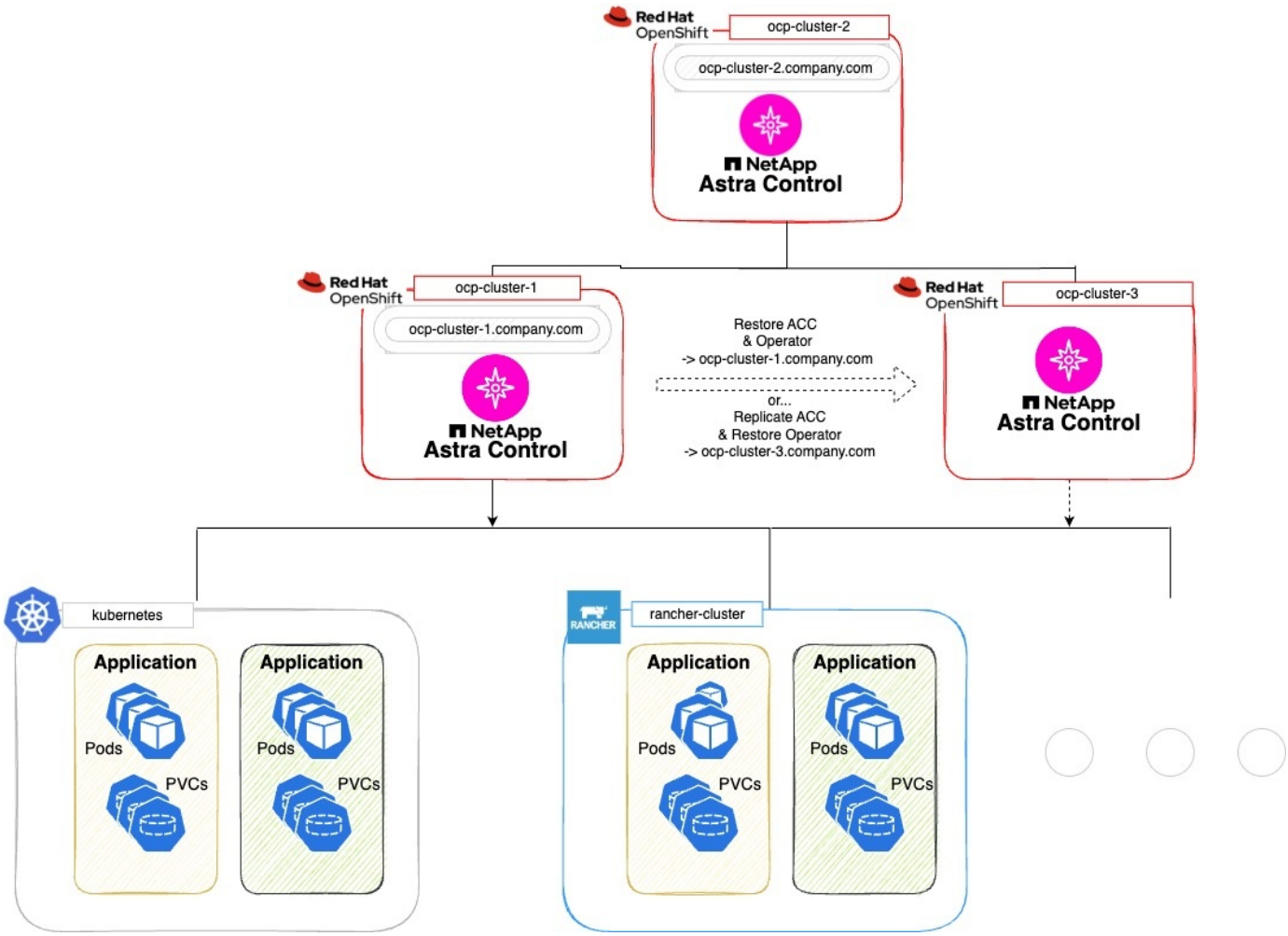
Prima di iniziare

Prima di impostare scenari di protezione per Astra Control Center, assicurarsi di disporre dei seguenti requisiti:

- **Un cluster Kubernetes che esegue l'istanza primaria Astra Control Center**: Questo cluster ospita l'istanza primaria Astra Control Center che gestisce i cluster di applicazioni.
- **Un secondo cluster Kubernetes dello stesso tipo di distribuzione Kubernetes del primario che esegue l'istanza secondaria di Astra Control Center**: Questo cluster ospita l'istanza di Astra Control Center che gestisce l'istanza primaria di Astra Control Center.
- **Un terzo cluster Kubernetes dello stesso tipo di distribuzione Kubernetes del primario**: Questo cluster ospiterà l'istanza ripristinata o replicata di Astra Control Center. Deve avere lo stesso namespace Astra Control Center disponibile che è attualmente distribuito nel primario. Ad esempio, se Astra Control Center viene implementato nello spazio dei nomi `netapp-acc` nel cluster di origine, lo spazio dei nomi `netapp-acc` Deve essere disponibile e non deve essere utilizzato da alcuna applicazione sul cluster Kubernetes di destinazione.
- **Bucket compatibili con S3**: Ogni istanza di Astra Control Center dispone di un bucket di storage a oggetti accessibile compatibile con S3.
- **Un bilanciatore di carico configurato**: Il bilanciatore di carico fornisce un indirizzo IP per Astra e deve avere connettività di rete ai cluster di applicazioni ed entrambi i bucket S3.
- **I cluster soddisfano i requisiti di Astra Control Center**: Ogni cluster utilizzato nella protezione Astra Control Center è conforme "Requisiti generali di Astra Control Center".

A proposito di questa attività

Queste procedure descrivono i passaggi necessari per ripristinare Astra Control Center in un nuovo cluster mediante uno dei due backup e ripristino oppure replica. I passaggi si basano sulla configurazione di esempio qui illustrata:



In questa configurazione di esempio, viene visualizzato quanto segue:

- **Un cluster Kubernetes che esegue l'istanza primaria Astra Control Center**:
  - Cluster OpenShift: `ocp-cluster-1`
  - Istanza primaria Astra Control Center: `ocp-cluster-1.company.com`
  - Questo cluster gestisce i cluster di applicazioni.
- **Il secondo cluster Kubernetes dello stesso tipo di distribuzione Kubernetes del primario che esegue l'istanza secondaria Astra Control Center**:
  - Cluster OpenShift: `ocp-cluster-2`
  - Istanza secondaria Astra Control Center: `ocp-cluster-2.company.com`
  - Questo cluster verrà utilizzato per eseguire il backup dell'istanza primaria di Astra Control Center o per configurare la replica su un cluster diverso (in questo esempio, il `ocp-cluster-3` cluster).
- **Un terzo cluster Kubernetes dello stesso tipo di distribuzione Kubernetes del primario che verrà utilizzato per le operazioni di ripristino**:
  - Cluster OpenShift: `ocp-cluster-3`
  - Terza istanza di Astra Control Center: `ocp-cluster-3.company.com`
  - Questo cluster verrà utilizzato per il ripristino di Astra Control Center o il failover della replica.

Idealmente, il cluster di applicazioni dovrebbe essere situato al di fuori dei tre cluster Astra Control Center, come illustrato dai cluster kuBoost e rancher nell'immagine precedente.

Non raffigurato nello schema:

- Tutti i cluster dispongono di backend ONTAP con Trident installato.
- In questa configurazione, i cluster OpenShift utilizzano MetalLB come bilanciatore del carico.
- Il controller dello snapshot e VolumeSnapshotClass vengono installati anche in tutti i cluster, come descritto nella "prerequisiti".

Opzione passaggio 1: Eseguire il backup e il ripristino di Astra Control Center

Questa procedura descrive i passaggi necessari per ripristinare Astra Control Center in un nuovo cluster utilizzando il backup e il ripristino.

In questo esempio, Astra Control Center è sempre installato in `netapp-acc` spazio dei nomi e l'operatore viene installato sotto `netapp-acc-operator` namespace.

Anche se non descritto, l'operatore di Astra Control Center può essere distribuito nello stesso namespace di Astra CR.

Prima di iniziare

- È stato installato Astra Control Center primario in un cluster.
- È stato installato Astra Control Center secondario su un cluster diverso.

Fasi

1. Gestire le applicazioni Astra Control Center primarie e il cluster di destinazione dall'istanza Astra Control Center secondaria (in esecuzione su `ocp-cluster-2` cluster):
   a. Accedere all'istanza secondaria di Astra Control Center.
   b. "Aggiungere il cluster Astra Control Center primario" (`ocp-cluster-1`).
   c. "Aggiungere il terzo cluster di destinazione" (`ocp-cluster-3`) che verrà utilizzato per il ripristino.
2. Gestire Astra Control Center e l'operatore Astra Control Center sul secondario Astra Control Center:
   a. Dalla pagina applicazioni, selezionare **Definisci**.
   b. Nella finestra **Definisci applicazione**, immettere il nome della nuova applicazione (`netapp-acc`).
   c. Scegli il cluster che esegue l'Astra Control Center primario (`ocp-cluster-1`) Dall'elenco a discesa **Cluster**.
   d. Scegliere `netapp-acc` Spazio dei nomi per Astra Control Center dall'elenco a discesa **namespace**.
   e. Nella pagina risorse cluster, selezionare **Includi risorse aggiuntive con ambito cluster**.
   f. Selezionare **Aggiungi regola di inclusione**.
   g. Selezionare queste voci, quindi selezionare **Aggiungi**:
      - Selettore etichette: <label name>
      - Gruppo: ApiExtensions.k8s.io
      - Versione: V1

- Tipo: CustomResourceDefinition

h. Confermare le informazioni sull'applicazione.

i. Selezionare **Definisci**.

Dopo aver selezionato **define**, ripetere il processo di definizione dell'applicazione per l'operatore `netapp-acc-operator`) e selezionare `netapp-acc-operator` Spazio dei nomi nella procedura guidata Definisci applicazione.

3. Eseguire il backup di Astra Control Center e dell'operatore:

a. Nell'Astra Control Center secondario, accedere alla pagina applicazioni selezionando la scheda applicazioni.

b. "Backup" L'applicazione Astra Control Center (`netapp-acc`).

c. "Backup" l'operatore (`netapp-acc-operator`).

4. Dopo aver eseguito il backup di Astra Control Center e dell'operatore, simulare uno scenario di disaster recovery (DR) di "Disinstallazione di Astra Control Center" dal cluster primario.

Astra Control Center verrà ripristinato in un nuovo cluster (il terzo cluster Kubernetes descritto in questa procedura) e utilizzerai lo stesso DNS del cluster primario per Astra Control Center appena installato.

5. Utilizzando l'Astra Control Center secondario, "ripristinare" L'istanza principale dell'applicazione Astra Control Center dal proprio backup:

a. Selezionare **applicazioni**, quindi selezionare il nome dell'applicazione Astra Control Center.

b. Dal menu Opzioni nella colonna azioni, selezionare **Ripristina**.

c. Scegliere **Restore to new namespaces** come tipo di ripristino.

d. Immettere il nome del ripristino (`netapp-acc`).

e. Scegliere il terzo cluster di destinazione (`ocp-cluster-3`).

f. Aggiornare lo spazio dei nomi di destinazione in modo che sia lo stesso spazio dei nomi dell'originale.

g. Nella pagina origine ripristino, selezionare il backup dell'applicazione che verrà utilizzato come origine di ripristino.

h. Selezionare **Ripristina utilizzando le classi di archiviazione originali**.

i. Selezionare **Ripristina tutte le risorse**.

j. Esaminare le informazioni di ripristino, quindi selezionare **Restore** (Ripristina) per avviare il processo di ripristino che ripristina Astra Control Center nel cluster di destinazione (`ocp-cluster-3`). Il ripristino è completo all'accesso dell'applicazione `available` stato.

6. Configurare Astra Control Center sul cluster di destinazione:

a. Aprire un terminale e collegarsi utilizzando kubeconfig al cluster di destinazione (`ocp-cluster-3`) Che contiene Astra Control Center ripristinato.

b. Verificare che il `ADDRESS` Nella configurazione Astra Control Center fa riferimento al nome DNS del sistema primario:

```
kubectl get acc -n netapp-acc
```

Risposta:

```
NAME  UUID                                   VERSION    ADDRESS
READY
astra 89f4fd47-0cf0-4c7a-a44e-43353dc96ba8 23.10.0-68 ocp-cluster-
1.company.com           True
```

a. Se il `ADDRESS` Nel campo della risposta sopra riportata non è presente l'FQDN dell'istanza primaria di Astra Control Center, aggiornare la configurazione per fare riferimento al DNS di Astra Control Center:

```
kubectl edit acc -n netapp-acc
```

i. Modificare il `astraAddress` sotto `spec:` All'FQDN (`ocp-cluster-1.company.com` In questo esempio) dell'istanza primaria Astra Control Center.

ii. Salvare la configurazione.

iii. Verificare che l'indirizzo sia stato aggiornato:

```
kubectl get acc -n netapp-acc
```

b. Accedere alla Ripristinare l'operatore Astra Control Center di questo documento per completare il processo di ripristino.

Opzione fase 1: Protezione di Astra Control Center con la replica

Questa procedura descrive i passaggi necessari per la configurazione "Replica di Astra Control Center" Per proteggere l'istanza primaria Astra Control Center.

In questo esempio, Astra Control Center è sempre installato in `netapp-acc` spazio dei nomi e l'operatore viene installato sotto `netapp-acc-operator` namespace.

Prima di iniziare

- È stato installato Astra Control Center primario in un cluster.
- È stato installato Astra Control Center secondario su un cluster diverso.

Fasi

1. Gestire l'applicazione Astra Control Center primaria e il cluster di destinazione dall'istanza Astra Control Center secondaria:
   a. Accedere all'istanza secondaria di Astra Control Center.
   b. "Aggiungere il cluster Astra Control Center primario" (`ocp-cluster-1`).
   c. "Aggiungere il terzo cluster di destinazione" (`ocp-cluster-3`) che verrà utilizzato per la replica.
2. Gestire Astra Control Center e l'operatore Astra Control Center sul secondario Astra Control Center:
   a. Selezionare **Cluster** e selezionare il cluster che contiene Astra Control Center primario (`ocp-cluster-1`).

b. Selezionare la scheda **spazi dei nomi**.

c. Selezionare `netapp-acc` e. `netapp-acc-operator` namespace.

d. Selezionare il menu azioni e selezionare **Definisci come applicazioni**.

e. Selezionare **Visualizza in applicazioni** per visualizzare le applicazioni definite.

3. Configurare i backend per la replica:

> La replica richiede che il cluster Astra Control Center primario e il cluster di destinazione (`ocp-cluster-3`) Utilizzare differenti backend di archiviazione ONTAP con peered. Dopo che ogni backend è stato sottoposto a peering e aggiunto ad Astra Control, il backend viene visualizzato nella scheda **scoperto** della pagina Backend.

a. "Aggiungere un backend con peered" Ad Astra Control Center sul cluster primario.

b. "Aggiungere un backend con peered" Ad Astra Control Center nel cluster di destinazione.

4. Configurare la replica:

a. Nella schermata applicazioni, selezionare `netapp-acc` applicazione.

b. Selezionare **Configura policy di replica**.

c. Selezionare `ocp-cluster-3` come cluster di destinazione.

d. Selezionare la classe di archiviazione.

e. Invio `netapp-acc` come namespace di destinazione.

f. Se necessario, modificare la frequenza di replica.

g. Selezionare **Avanti**.

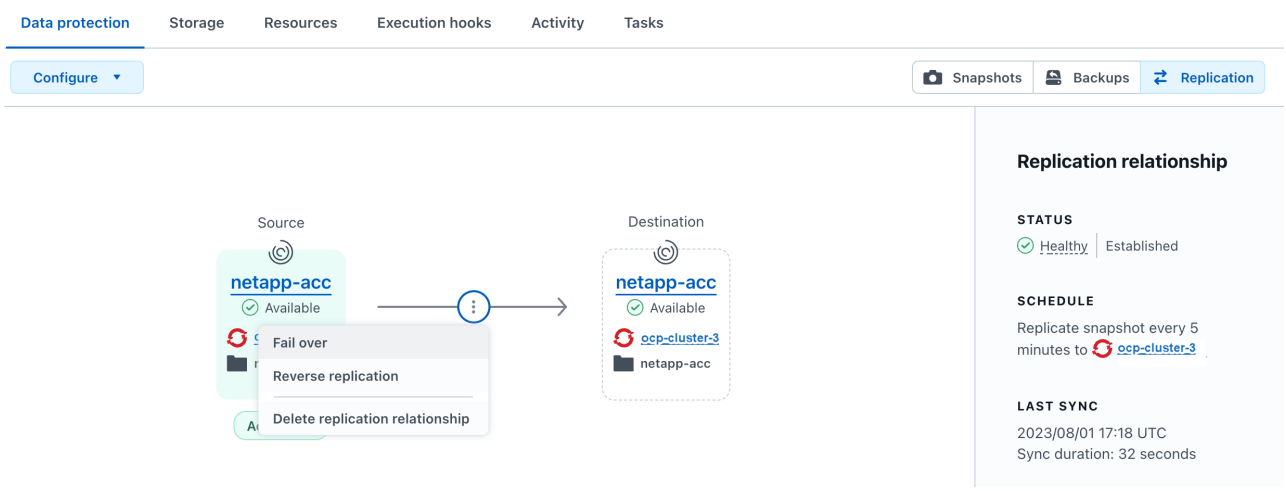
h. Verificare che la configurazione sia corretta e selezionare **Salva**.

Il rapporto di replica passa da `Establishing` a. `Established`. Quando è attiva, la replica viene eseguita ogni cinque minuti fino all'eliminazione della configurazione della replica.

5. Esegui il failover della replica nell'altro cluster se il sistema primario è danneggiato o non più accessibile:

> Assicurarsi che nel cluster di destinazione non sia installato Astra Control Center per garantire un failover corretto.

a. Selezionare l'icona ellissi verticali e selezionare **failover**.



b. Confermare i dettagli e selezionare **failover** per avviare il processo di failover.

   Lo stato della relazione di replica cambia in `Failing over` e poi `Failed over` al termine dell'operazione.

6. Completare la configurazione di failover:

   a. Aprire un terminale e connettersi utilizzando il kubeconfig del terzo quadro strumenti (`ocp-cluster-3`). In questo cluster è ora installato Astra Control Center.

   b. Determinare l'FQDN Astra Control Center sul terzo cluster (`ocp-cluster-3`).

   c. Aggiornare la configurazione per fare riferimento al DNS di Astra Control Center:

```
kubectl edit acc -n netapp-acc
```

      i. Modificare il `astraAddress` sotto `spec:` Con l'FQDN (`ocp-cluster-3.company.com`) del terzo cluster di destinazione.

      ii. Salvare la configurazione.

      iii. Verificare che l'indirizzo sia stato aggiornato:

```
kubectl get acc -n netapp-acc
```

   d. confermare la presenza di tutti i CRD traefik richiesti:

```
kubectl get crds | grep traefik
```

   CRDS traefik richiesti:

```
ingressroutes.traefik.containo.us
ingressroutes.traefik.io
ingressroutetcps.traefik.containo.us
ingressroutetcps.traefik.io
ingressrouteudps.traefik.containo.us
ingressrouteudps.traefik.io
middlewares.traefik.containo.us
middlewares.traefik.io
middlewaretcps.traefik.containo.us
middlewaretcps.traefik.io
serverstransports.traefik.containo.us
serverstransports.traefik.io
tlsoptions.traefik.containo.us
tlsoptions.traefik.io
tIsstores.traefik.containo.us
tIsstores.traefik.io
traefikservices.traefik.containo.us
traefikservices.traefik.io
```

a. Se alcuni dei CRD sopra elencati non sono presenti:
   i. Passare a. "documentazione di traefik".
   ii. Copiare l'area "Definitions" (definizioni) in un file.
   iii. Applica modifiche:

```
kubectl apply -f <file name>
```

   iv. Riavvia traefik:

```
kubectl get pods -n netapp-acc | grep -e "traefik" | awk '{print
$1}' | xargs kubectl delete pod -n netapp-acc
```

b. Accedere alla Ripristinare l'operatore Astra Control Center di questo documento per completare il processo di ripristino.

Fase 2: Ripristinare l'operatore Astra Control Center

Utilizzando Astra Control Center secondario, ripristinare l'operatore Astra Control Center primario dal backup. Lo spazio dei nomi di destinazione deve essere lo stesso dello spazio dei nomi di origine. Nel caso in cui Astra Control Center sia stato eliminato dal cluster di origine primario, i backup esisteranno ancora per eseguire la stessa procedura di ripristino.

Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome dell'applicazione operatore (`netapp-acc-operator`).

2. Dal menu Opzioni nella colonna azioni, selezionare **Ripristina**
3. Scegliere **Restore to new namespaces** come tipo di ripristino.
4. Scegliere il terzo cluster di destinazione (`ocp-cluster-3`).
5. Modificare lo spazio dei nomi in modo che sia lo stesso dello spazio dei nomi associato al cluster di origine primario (`netapp-acc-operator`).
6. Selezionare il backup eseguito in precedenza come origine di ripristino.
7. Selezionare **Ripristina utilizzando le classi di archiviazione originali**.
8. Selezionare **Ripristina tutte le risorse**.
9. Esaminare i dettagli, quindi fare clic su **Ripristina** per avviare il processo di ripristino.

   La pagina Applications (applicazioni) mostra l'operatore Astra Control Center ripristinato nel terzo cluster di destinazione (`ocp-cluster-3`). Al termine del processo, lo stato indica come `Available`. Entro dieci minuti, l'indirizzo DNS dovrebbe risolversi nella pagina.

Risultato

Astra Control Center, i suoi cluster registrati e le applicazioni gestite con snapshot e backup sono ora disponibili nel terzo cluster di destinazione (`ocp-cluster-3`). Tutti i criteri di protezione dell'originale sono presenti anche nella nuova istanza. Puoi continuare a eseguire backup e snapshot pianificati o on-demand.

Risoluzione dei problemi

Determinare lo stato del sistema e se i processi di protezione hanno avuto esito positivo.

- **I pod non sono in esecuzione**: Verificare che tutti i pod siano attivi e in esecuzione:

  ```
  kubectl get pods -n netapp-acc
  ```

  Se alcuni pod sono in `CrashLookBackOff` specificare, riavviarli e dovrebbero passare a. `Running` stato.

- **Confermare lo stato del sistema**: Verificare che il sistema Astra Control Center sia attivo `ready` stato:

  ```
  kubectl get acc -n netapp-acc
  ```

  Risposta:

  ```
  NAME  UUID                                   VERSION    ADDRESS
  READY
  astra 89f4fd47-0cf0-4c7a-a44e-43353dc96ba8 23.10.0-68 ocp-cluster-
  1.company.com           True
  ```

- **Conferma lo stato di distribuzione**: Mostra le informazioni di distribuzione di Astra Control Center per confermare `Deployment State` è `Deployed`.

```
kubectl describe acc astra -n netapp-acc
```

- **L'interfaccia utente di Astra Control Center ripristinata restituisce un errore 404**: Se questo accade quando si seleziona `AccTraefik` come opzione di ingresso, controllare CRD traefik per assicurarsi che siano tutti installati.

Monitorare 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 puoi eseguire il drill-down da ciascuno di essi. 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.

Sezione applicazioni

La sezione **applicazioni** 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.

Visualizzare lo stato dei cluster e gestire le classi di storage

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. È inoltre possibile modificare la classe di storage predefinita per i cluster gestiti.

Visualizzare lo stato e i dettagli del cluster

È possibile visualizzare i dettagli del cluster, ad esempio la 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.

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

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.

Modificare la classe di storage predefinita

È possibile modificare la classe di storage predefinita per un cluster. Quando Astra Control gestisce un cluster, tiene traccia della classe di storage predefinita del cluster.

> Non modificare la classe di storage utilizzando i comandi kubectl. Utilizzare questa procedura. Astra Control ripristinerà le modifiche se effettuate utilizzando kubectl.

Fasi

1. Nell'interfaccia utente Web di Astra Control Center, selezionare **Clusters**.
2. Nella pagina **Clusters**, selezionare il cluster che si desidera modificare.
3. Selezionare la scheda **Storage**.
4. Selezionare la categoria **classi di storage**.

5. Selezionare il menu **azioni** per la classe di storage che si desidera impostare come predefinita.
6. Selezionare **Imposta come predefinito**.

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

Dopo aver iniziato a gestire un'app, Astra Control fornisce dettagli sull'app che ti permette di identificarne lo stato di comunicazione (se Astra Control è in grado di comunicare con l'app), il suo stato di protezione (se è completamente protetto in caso di guasto), i pod, lo storage persistente e altro ancora.

Fasi

1. Nell'interfaccia utente di Astra Control Center, selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Esaminare le informazioni.

   Stato dell'app

   Fornisce uno stato che riflette se Astra Control può comunicare con l'applicazione.

   - **App Protection Status**: 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.
   - **Data Protection**: 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 **applicazioni** sotto **Riepilogo risorse**, è possibile selezionare le applicazioni gestite, che consentono di accedere alla pagina **applicazioni**. Una volta visualizzata la pagina **applicazioni**, seguire la procedura descritta in precedenza.

Gestisci il tuo account

Gestire utenti e ruoli locali

È possibile aggiungere, rimuovere e modificare gli utenti dell'installazione di Astra Control Center utilizzando l'interfaccia utente di Astra Control. È possibile utilizzare l'interfaccia utente di Astra Control o. "API di controllo Astra" per gestire gli utenti.

È inoltre possibile utilizzare LDAP per eseguire l'autenticazione per gli utenti selezionati.

Utilizzare LDAP

LDAP è un protocollo standard di settore per l'accesso alle informazioni di directory distribuite e una scelta popolare per l'autenticazione aziendale. È possibile collegare Astra Control Center a un server LDAP per eseguire l'autenticazione per gli utenti Astra Control selezionati. Ad alto livello, la configurazione prevede l'integrazione di Astra con LDAP e la definizione degli utenti e dei gruppi Astra Control corrispondenti alle definizioni LDAP. È possibile utilizzare l'API Astra Control o l'interfaccia utente Web per configurare l'autenticazione LDAP e gli utenti e i gruppi LDAP. Per ulteriori informazioni, consultare la seguente documentazione:

- "Utilizzare l'API Astra Control per gestire l'autenticazione remota e gli utenti"
- "Utilizzare l'interfaccia utente di Astra Control per gestire utenti e gruppi remoti"
- "Utilizzare l'interfaccia utente di Astra Control per gestire l'autenticazione remota"

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**, selezionare **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 per il ruolo Viewer e può gestire app e cluster, annullare la gestione delle app ed eliminare snapshot e 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. Per aggiungere vincoli a un utente con ruolo membro o visualizzatore, attivare la casella di controllo **limita ruolo ai vincoli**.

Per ulteriori informazioni sull'aggiunta di vincoli, fare riferimento a. "Gestire utenti e ruoli locali".

7. Selezionare **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. Selezionare l'icona User (utente) nella parte superiore destra della schermata.
2. Selezionare **Profilo**.
3. Dal menu Opzioni nella colonna **azioni** e selezionare **Modifica password**.
4. Immettere una password conforme ai requisiti.
5. Immettere nuovamente la password per confermare.
6. Selezionare **Cambia 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**, selezionare **account**.
2. Selezionare l'elenco a discesa **azioni**.
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. Selezionare **Ripristina password**.

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**, selezionare **account**.
2. Nella scheda **utenti**, selezionare la casella di controllo nella riga di ciascun utente che si desidera rimuovere.
3. Dal menu Options (Opzioni) nella colonna **Actions** (azioni), selezionare **Remove user/s** (Rimuovi utenti).
4. Quando richiesto, confermare l'eliminazione digitando la parola "remove", quindi selezionare **Yes, Remove**

User (Sì, Rimuovi utente).

Risultato

Astra Control Center rimuove l'utente dall'account.

Gestire i ruoli

È possibile gestire i ruoli aggiungendo vincoli dello spazio dei nomi e limitando i ruoli utente a tali vincoli. In questo modo è possibile controllare l'accesso alle risorse all'interno dell'organizzazione. È possibile utilizzare l'interfaccia utente di Astra Control o. "API di controllo Astra" per gestire i ruoli.

Aggiungere un vincolo dello spazio dei nomi a un ruolo

Un utente Admin o Owner può aggiungere vincoli di spazio dei nomi ai ruoli Member o Viewer.

Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **utenti**.
3. Nella colonna **azioni**, selezionare il pulsante di menu per un utente con ruolo membro o visualizzatore.
4. Selezionare **Modifica ruolo**.
5. Attivare la casella di controllo **limita ruolo ai vincoli**.

   La casella di controllo è disponibile solo per i ruoli Member o Viewer. È possibile selezionare un ruolo diverso dall'elenco a discesa **ruolo**.

6. Selezionare **Aggiungi vincolo**.

   È possibile visualizzare l'elenco dei vincoli disponibili in base allo spazio dei nomi o all'etichetta dello spazio dei nomi.

7. Nell'elenco a discesa **tipo di vincolo**, selezionare **spazio dei nomi Kubernetes** o **etichetta dello spazio dei nomi Kubernetes** a seconda della configurazione degli spazi dei nomi.
8. Selezionare uno o più spazi dei nomi o etichette dall'elenco per comporre un vincolo che limiti i ruoli a tali spazi dei nomi.
9. Selezionare **Conferma**.

   La pagina **Modifica ruolo** visualizza l'elenco dei vincoli scelti per questo ruolo.

10. Selezionare **Conferma**.

    Nella pagina **account**, è possibile visualizzare i vincoli per qualsiasi ruolo membro o visualizzatore nella colonna **ruolo**.

> Se si abilitano i vincoli per un ruolo e si seleziona **Conferma** senza aggiungere alcun vincolo, il ruolo viene considerato con restrizioni complete (al ruolo viene negato l'accesso a tutte le risorse assegnate agli spazi dei nomi).

Rimuovere un vincolo dello spazio dei nomi da un ruolo

Un utente Admin o Owner può rimuovere un vincolo dello spazio dei nomi da un ruolo.

Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **utenti**.
3. Nella colonna **azioni**, selezionare il pulsante di menu per un utente con ruolo membro o visualizzatore con vincoli attivi.
4. Selezionare **Modifica ruolo**.

   La finestra di dialogo **Modifica ruolo** visualizza i vincoli attivi per il ruolo.

5. Selezionare la **X** a destra del vincolo da rimuovere.
6. Selezionare **Conferma**.

Per ulteriori informazioni

- "Ruoli e spazi dei nomi degli utenti"

Gestire l'autenticazione remota

LDAP è un protocollo standard di settore per l'accesso alle informazioni di directory distribuite e una scelta popolare per l'autenticazione aziendale. È possibile collegare Astra Control Center a un server LDAP per eseguire l'autenticazione per gli utenti Astra Control selezionati.

Ad alto livello, la configurazione prevede l'integrazione di Astra con LDAP e la definizione degli utenti e dei gruppi Astra Control corrispondenti alle definizioni LDAP. È possibile utilizzare l'API Astra Control o l'interfaccia utente Web per configurare l'autenticazione LDAP e gli utenti e i gruppi LDAP.

> Astra Control Center utilizza l'attributo user login, configurato quando l'autenticazione remota è abilitata, per cercare e tenere traccia degli utenti remoti. In questo campo deve esistere un attributo di un indirizzo e-mail ("mail") o di un nome principale utente ("userPrincipalName") per qualsiasi utente remoto che si desidera visualizzare in Astra Control Center. Questo attributo viene utilizzato come nome utente in Astra Control Center per l'autenticazione e la ricerca di utenti remoti.

Aggiungere un certificato per l'autenticazione LDAPS

Aggiungere il certificato TLS privato per il server LDAP in modo che Astra Control Center possa autenticarsi con il server LDAP quando si utilizza una connessione LDAPS. Questa operazione deve essere eseguita una sola volta o alla scadenza del certificato installato.

Fasi

1. Vai a **account**.
2. Selezionare la scheda **certificati**.
3. Selezionare **Aggiungi**.
4. Caricare il `.pem` archiviare o incollare il contenuto del file dagli appunti.
5. Selezionare la casella di controllo **attendibile**.
6. Selezionare **Aggiungi certificato**.

Abilitare l'autenticazione remota

È possibile attivare l'autenticazione LDAP e configurare la connessione tra Astra Control e il server LDAP remoto.

Prima di iniziare

Se si intende utilizzare LDAPS, assicurarsi che il certificato TLS privato per il server LDAP sia installato in Astra Control Center in modo che Astra Control Center possa autenticarsi con il server LDAP. Vedere Aggiungere un certificato per l'autenticazione LDAPS per istruzioni.

Fasi

1. Accedere a **account > connessioni**.
2. Nel riquadro **Remote Authentication**, selezionare il menu di configurazione.
3. Selezionare **Connect**.
4. Inserire l'indirizzo IP del server, la porta e il protocollo di connessione preferito (LDAP o LDAPS).

> Come Best practice, utilizzare LDAPS per la connessione con il server LDAP. È necessario installare il certificato TLS privato del server LDAP in Astra Control Center prima di connettersi a LDAPS.

5. Inserire le credenziali dell'account di servizio nel formato e-mail (administrator@example.com). Astra Control utilizza queste credenziali per la connessione con il server LDAP.
6. Nella sezione **corrispondenza utente**, procedere come segue:
   a. Inserire il DN di base e un filtro di ricerca utente appropriato da utilizzare per recuperare le informazioni utente dal server LDAP.
   b. (Facoltativo) se la directory utilizza l'attributo di accesso utente `userPrincipalName` invece di `mail`, invio `userPrincipalName` Nell'attributo corretto nel campo **attributo di accesso utente**.
7. Nella sezione **corrispondenza gruppo**, immettere il DN della base di ricerca gruppo e un filtro di ricerca gruppo personalizzato appropriato.

> Assicurarsi di utilizzare il nome distinto (DN) di base corretto e un filtro di ricerca appropriato per **corrispondenza utente** e **corrispondenza gruppo**. Il DN di base indica ad Astra Control a quale livello della struttura di directory avviare la ricerca e il filtro di ricerca limita le parti della struttura di directory da cui Astra Control esegue la ricerca.

8. Selezionare **Invia**.

Risultato

Lo stato del riquadro **Remote Authentication** (autenticazione remota) passa a **Pending** (in sospeso), quindi a **Connected** (connesso) quando viene stabilita la connessione al server LDAP.

Disattiva autenticazione remota

È possibile disattivare temporaneamente una connessione attiva al server LDAP.

> Quando si disattiva una connessione a un server LDAP, vengono salvate tutte le impostazioni e vengono conservati tutti gli utenti e i gruppi remoti aggiunti ad Astra Control da tale server LDAP. È possibile riconnettersi a questo server LDAP in qualsiasi momento.

Fasi

1. Accedere a **account > connessioni**.
2. Nel riquadro **Remote Authentication**, selezionare il menu di configurazione.
3. Selezionare **Disable** (Disattiva).

Risultato

Lo stato del riquadro **Remote Authentication** passa a **Disabled**. Tutte le impostazioni di autenticazione remota, gli utenti remoti e i gruppi remoti vengono preservati e la connessione può essere riattivata in qualsiasi momento.

Modificare le impostazioni di autenticazione remota

Se la connessione al server LDAP è stata disattivata o il pannello **Remote Authentication** è in stato "Connection error" (errore di connessione), è possibile modificare le impostazioni di configurazione.

> Non è possibile modificare l'URL o l'indirizzo IP del server LDAP quando il pannello **Remote Authentication** (autenticazione remota) è in stato "Disabled" (Disattivato). È necessario Disconnettere l'autenticazione remota prima di tutto.

Fasi

1. Accedere a **account > connessioni**.
2. Nel riquadro **Remote Authentication**, selezionare il menu di configurazione.
3. Selezionare **Modifica**.
4. Apportare le modifiche necessarie e selezionare **Modifica**.

Disconnettere l'autenticazione remota

È possibile disconnettersi da un server LDAP e rimuovere le impostazioni di configurazione da Astra Control.

> Se si è un utente LDAP e si disconnette, la sessione si concluderà immediatamente Quando ci si disconnette dal server LDAP, tutte le impostazioni di configurazione per quel server LDAP vengono rimosse da Astra Control, così come tutti gli utenti e i gruppi remoti che sono stati aggiunti da quel server LDAP.

Fasi

1. Accedere a **account > connessioni**.
2. Nel riquadro **Remote Authentication**, selezionare il menu di configurazione.
3. Selezionare **Disconnect**.

Risultato

Lo stato del riquadro **Remote Authentication** (autenticazione remota) passa a **Disconnected** (disconnesso). Le impostazioni di autenticazione remota, gli utenti remoti e i gruppi remoti vengono rimossi da Astra Control.

Gestire utenti e gruppi remoti

Se è stata attivata l'autenticazione LDAP sul sistema Astra Control, è possibile cercare utenti e gruppi LDAP e includerli negli utenti approvati del sistema.

Aggiungere un utente remoto

Gli account Owner e gli amministratori possono aggiungere utenti remoti ad Astra Control. Astra Control Center supporta fino a 10,000 utenti remoti LDAP.

> Astra Control Center utilizza l'attributo user login, configurato quando l'autenticazione remota è abilitata, per cercare e tenere traccia degli utenti remoti. In questo campo deve esistere un attributo di un indirizzo e-mail ("mail") o di un nome principale utente ("userPrincipalName") per qualsiasi utente remoto che si desidera visualizzare in Astra Control Center. Questo attributo viene utilizzato come nome utente in Astra Control Center per l'autenticazione e la ricerca di utenti remoti.

> Non è possibile aggiungere un utente remoto se nel sistema esiste già un utente locale con lo stesso indirizzo e-mail (basato sull'attributo "mail" o "nome principale utente"). Per aggiungere l'utente come utente remoto, eliminare prima l'utente locale dal sistema.

Fasi

1. Accedere all'area **account**.
2. Selezionare la scheda **utenti e gruppi**.
3. All'estrema destra della pagina, selezionare **utenti remoti**.
4. Selezionare **Aggiungi**.
5. In alternativa, cercare un utente LDAP inserendo l'indirizzo e-mail dell'utente nel campo **Filtra per email**.
6. Selezionare uno o più utenti dall'elenco.
7. Assegnare un ruolo all'utente.

   > Se si assegnano ruoli diversi a un utente e al gruppo dell'utente, il ruolo più permissivo ha la precedenza.

8. Facoltativamente, assegnare uno o più vincoli dello spazio dei nomi a questo utente e selezionare **limita ruolo ai vincoli** per applicarli. È possibile aggiungere un nuovo vincolo dello spazio dei nomi selezionando **Aggiungi vincolo**.

   > Quando a un utente vengono assegnati ruoli multipli tramite l'appartenenza al gruppo LDAP, i limiti nel ruolo più permissivo sono gli unici che hanno effetto. Ad esempio, se un utente con un ruolo Viewer locale unisce tre gruppi associati al ruolo Member, la somma dei vincoli dei ruoli Member ha effetto e tutti i vincoli del ruolo Viewer vengono ignorati.

9. Selezionare **Aggiungi**.

Risultato

Il nuovo utente viene visualizzato nell'elenco degli utenti remoti. In questo elenco, è possibile visualizzare i vincoli attivi sull'utente e gestire l'utente dal menu **azioni**.

Aggiungere un gruppo remoto

Per aggiungere più utenti remoti contemporaneamente, gli account Owners e gli amministratori possono aggiungere gruppi remoti ad Astra Control. Quando si aggiunge un gruppo remoto, tutti gli utenti remoti di tale gruppo sono disponibili per accedere ad Astra Control e ereditano lo stesso ruolo del gruppo.

Astra Control Center supporta fino a 5,000 gruppi remoti LDAP.

Fasi

1. Accedere all'area **account**.
2. Selezionare la scheda **utenti e gruppi**.
3. All'estrema destra della pagina, selezionare **gruppi remoti**.
4. Selezionare **Aggiungi**.

   In questa finestra, è possibile visualizzare un elenco dei nomi comuni e dei nomi distinti dei gruppi LDAP recuperati da Astra Control.

5. In alternativa, cercare un gruppo LDAP inserendo il nome comune del gruppo nel campo **Filtra per nome comune**.
6. Selezionare uno o più gruppi dall'elenco.
7. Assegnare un ruolo ai gruppi.

   Il ruolo selezionato viene assegnato a tutti gli utenti di questo gruppo. Se si assegnano ruoli diversi a un utente e al gruppo dell'utente, il ruolo più permissivo ha la precedenza.

8. Facoltativamente, assegnare uno o più vincoli dello spazio dei nomi a questo gruppo e selezionare **limita ruolo ai vincoli** per applicarli. È possibile aggiungere un nuovo vincolo dello spazio dei nomi selezionando **Aggiungi vincolo**.

   Quando a un utente vengono assegnati ruoli multipli tramite l'appartenenza al gruppo LDAP, i limiti nel ruolo più permissivo sono gli unici che hanno effetto. Ad esempio, se un utente con un ruolo Viewer locale unisce tre gruppi associati al ruolo Member, la somma dei vincoli dei ruoli Member ha effetto e tutti i vincoli del ruolo Viewer vengono ignorati.

9. Selezionare **Aggiungi**.

Risultato

Il nuovo gruppo viene visualizzato nell'elenco dei gruppi remoti. Gli utenti remoti di questo gruppo non vengono visualizzati nell'elenco degli utenti remoti fino a quando ciascun utente remoto non effettua l'accesso. In questo elenco, è possibile visualizzare i dettagli sul gruppo e gestire il gruppo dal menu **azioni**.

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.

È possibile gestire queste notifiche dall'alto a destra dell'interfaccia:

Fasi

1. Selezionare il numero di notifiche non lette in alto a destra.

2. Esaminare le notifiche, quindi selezionare **Contrassegna come letto** o **Mostra tutte le notifiche**.

   Se si seleziona **Mostra tutte le notifiche**, viene caricata la pagina Notifiche.

3. Nella pagina **Notifiche**, visualizzare le notifiche, selezionare quelle che si desidera contrassegnare come lette, selezionare **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, fare riferimento a. "Aggiungere un cluster Kubernetes".

> Se si crea il proprio file kubeconfig, si dovrebbe definire solo **un** elemento di contesto al suo interno. Fare riferimento a. "Documentazione Kubernetes" per informazioni sulla creazione di file kubeconfig.

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. Selezionare **account**.
2. Selezionare la scheda **credenziali**.
3. Selezionare il menu Opzioni nella colonna **Stato** per le credenziali che si desidera rimuovere.
4. Selezionare **Rimuovi**.
5. Digitare la parola "remove" per confermare l'eliminazione, quindi selezionare **Sì, Rimuovi credenziale**.

Risultato

Astra Control Center rimuove le credenziali dall'account.

Monitorare l'attività dell'account

Puoi visualizzare i dettagli delle attività nel tuo account Astra Control. Ad esempio, quando sono stati invitati nuovi utenti, quando è stato aggiunto un cluster o quando è

stata acquisita una snapshot. È inoltre possibile esportare l'attività dell'account in un file CSV.

Se gestisci i cluster Kubernetes da Astra Control e Astra Control è connesso a Cloud Insights, Astra Control invia i registri degli eventi a Cloud Insights. Le informazioni di log, incluse le informazioni sull'implementazione del pod e sugli allegati PVC, vengono visualizzate nel registro delle attività di controllo Astra. Utilizza queste informazioni per identificare eventuali problemi sui cluster Kubernetes che stai gestendo.

Visualizza tutte le attività dell'account in Astra Control

1. Selezionare **Activity** (attività).
2. Utilizza i filtri per restringere l'elenco delle attività o utilizza la casella di ricerca per trovare esattamente ciò che stai cercando.
3. Selezionare **Export to CSV** (Esporta in CSV) per scaricare l'attività dell'account in un file CSV.

Visualizzare l'attività dell'account per un'applicazione specifica

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Selezionare **Activity** (attività).

Visualizzare l'attività dell'account per i cluster

1. Selezionare **Clusters**, quindi il nome del cluster.
2. Selezionare **Activity** (attività).

Intraprendere azioni per risolvere gli eventi che richiedono attenzione

1. Selezionare **Activity** (attività).
2. Selezionare un evento che richiede attenzione.
3. Selezionare l'opzione a discesa **take action**.

   Da questo elenco è possibile visualizzare le possibili azioni correttive da intraprendere, visualizzare la documentazione relativa al problema e ottenere supporto per risolvere il problema.

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 di Astra Control Center o. "API di controllo Astra" per aggiornare una licenza esistente.

Fasi

1. Accedere a. "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**, selezionare il 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.

Per ulteriori informazioni

- "Licenza Astra Control Center"

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.

Utilizza uno dei seguenti provider di bucket Amazon Simple Storage Service (S3):

- NetApp ONTAP S3
- NetApp StorageGRID S3
- Microsoft Azure
- Generico S3

> Amazon Web Services (AWS) e Google Cloud Platform (GCP) utilizzano il tipo di bucket S3 generico.

> 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 rivendicano il supporto S3 di Amazon.

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 Control, vedere "Astra Automation e informazioni API".

È possibile eseguire queste attività relative alla gestione dei bucket:

- "Aggiungi un bucket"

- Modificare un bucket
- Impostare il bucket predefinito
- Ruotare o rimuovere le credenziali bucket
- Rimuovere una benna

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.

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 bucket provider corretto e fornire le credenziali corrette per tale provider. Ad esempio, l'interfaccia utente accetta come tipo NetApp ONTAP S3 e accetta le credenziali StorageGRID; tuttavia, questo causerà l'errore di tutti i backup e ripristini futuri dell'applicazione che utilizzano questo bucket. Vedere "Note di rilascio".

Fasi

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

   Impossibile modificare il tipo di bucket.

4. Selezionare **Aggiorna**.

Impostare il bucket predefinito

Quando si esegue un clone tra i cluster, Astra Control richiede un bucket predefinito. Seguire questi passaggi per impostare un bucket predefinito per tutti i cluster.

Fasi

1. Accedere a **istanze cloud**.
2. Selezionare il menu nella colonna **azioni** per l'istanza di cloud nell'elenco.
3. Selezionare **Modifica**.
4. Nell'elenco **bucket**, selezionare il bucket che si desidera impostare come predefinito.
5. Selezionare **Salva**.

Ruotare o rimuovere le credenziali bucket

Astra Control utilizza le credenziali bucket per ottenere l'accesso e fornire chiavi segrete per un bucket S3 in modo che Astra Control Center possa comunicare con il bucket.

Ruotare le credenziali del bucket

Se si ruotano le credenziali, ruotarle durante una finestra di manutenzione quando non sono in corso backup (pianificati o on-demand).

Procedura per modificare e ruotare le credenziali

1. Dalla barra di navigazione a sinistra, selezionare **Bucket**.
2. Dal menu Opzioni nella colonna **azioni**, selezionare **Modifica**.
3. Creare la nuova credenziale.
4. Selezionare **Aggiorna**.

Rimuovere le credenziali bucket

È necessario rimuovere le credenziali bucket solo se sono state applicate nuove credenziali a un bucket o se il bucket non è più utilizzato attivamente.

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. Non rimuovere queste credenziali se il bucket è in uso, in quanto ciò potrebbe causare errori di backup e indisponibilità del backup.

Se si rimuovono le credenziali bucket attive, vedere "risoluzione dei problemi relativi alla rimozione delle credenziali bucket".

Per istruzioni su come rimuovere le credenziali S3 utilizzando l'API Astra Control, vedere "Astra Automation e informazioni API".

Rimuovere una benna

È possibile rimuovere un bucket che non è più in uso o che non è integro. Questa operazione può essere utile per mantenere la configurazione dell'archivio di oggetti semplice e aggiornata.

- Non è possibile rimuovere un bucket predefinito. Se si desidera rimuovere tale bucket, selezionare prima un altro bucket come predefinito.
- Non è possibile rimuovere un bucket WORM (Write Once Read Many) prima che il periodo di conservazione del cloud provider del bucket sia scaduto. Le benne A VITE SENZA FINE sono contrassegnate con "bloccate" accanto al nome della benna.

- Non è possibile rimuovere un bucket predefinito. Se si desidera rimuovere tale bucket, selezionare prima un altro bucket come predefinito.

Prima di iniziare

- Prima di iniziare, verificare che non vi siano backup in esecuzione o completati per questo bucket.
- È necessario verificare che il bucket non venga utilizzato in alcuna policy di protezione attiva.

In tal caso, non sarà possibile continuare.

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Bucket**.
2. Dal menu **azioni**, selezionare **Rimuovi**.

Astra Control garantisce innanzitutto che non vi siano policy di pianificazione che utilizzano il bucket per i backup e che non vi siano backup attivi nel bucket che si sta per rimuovere.

3. Digitare "remove" per confermare l'azione.
4. Selezionare **Sì, Rimuovi bucket**.

Trova ulteriori informazioni

- "Utilizzare l'API di controllo 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 Control, 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
- Modificare i dettagli dell'autenticazione back-end dello storage
- Gestire un backend di storage rilevato
- Annullare la gestione di un backend di storage
- Rimuovere 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 il pannello Storage backend della dashboard 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

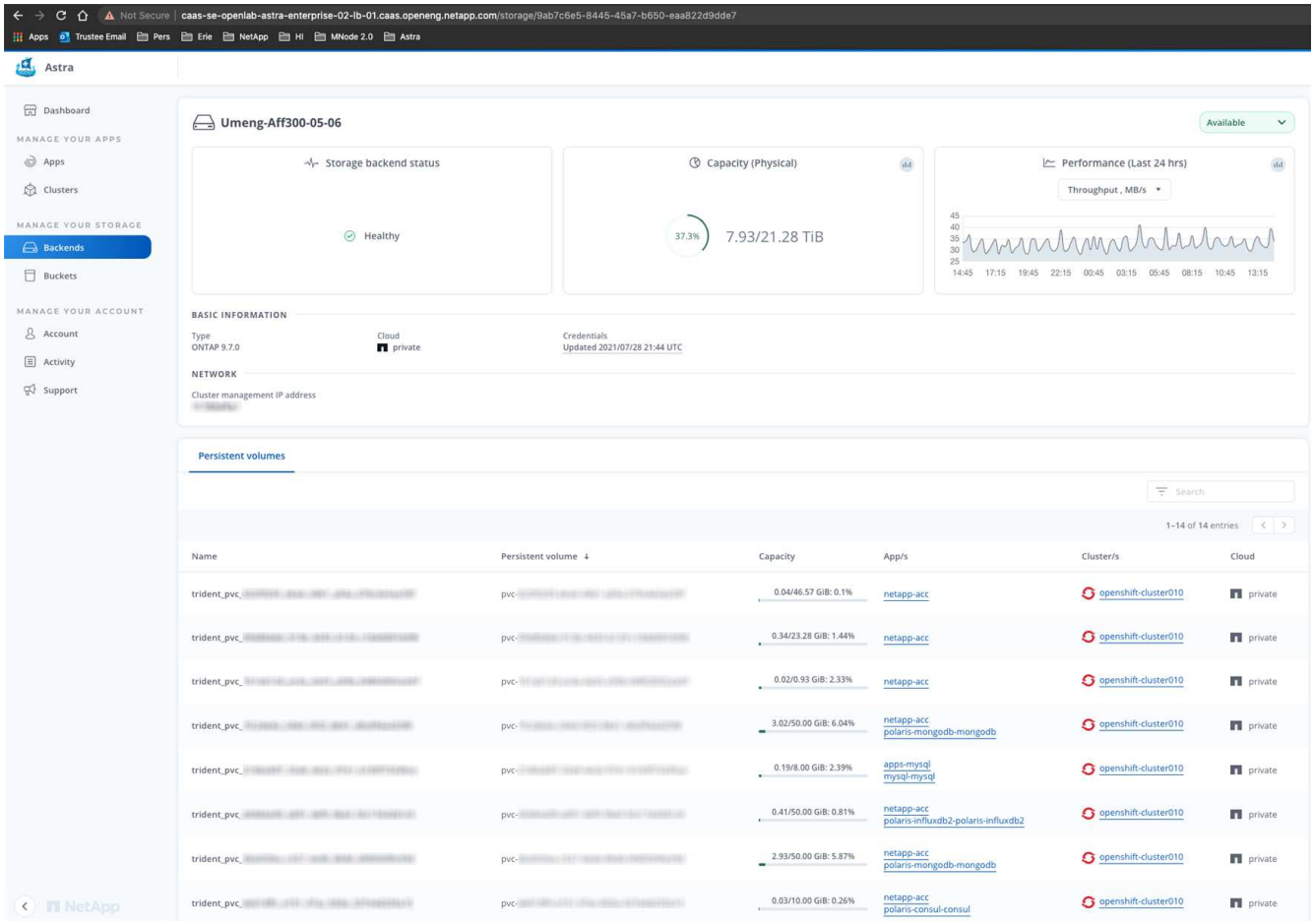
Visualizza informazioni sullo stato, la capacità e le performance del back-end (throughput IOPS e/o latenza).

È possibile visualizzare i volumi utilizzati dalle applicazioni Kubernetes, che vengono memorizzati in un backend di storage selezionato. Con Cloud Insights, è possibile visualizzare ulteriori informazioni. Vedere "Documentazione Cloud Insights".

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, selezionare l'icona **Cloud Insights** accanto all'immagine delle metriche.

Modificare i dettagli dell'autenticazione back-end dello storage

Centro di controllo Astra offre due modalità di autenticazione di un backend ONTAP.

- **Autenticazione basata su credenziali**: Nome utente e password di un utente ONTAP con le autorizzazioni richieste. È necessario utilizzare un ruolo di accesso di sicurezza predefinito, ad esempio admin, per garantire la massima compatibilità con le versioni di ONTAP.

- **Autenticazione basata su certificato**: Il centro di controllo Astra può anche comunicare con un cluster ONTAP utilizzando un certificato installato sul back-end. Utilizzare il certificato client, la chiave e il certificato CA attendibile, se utilizzato (consigliato).

È possibile aggiornare i backend esistenti per passare da un tipo di autenticazione a un altro metodo. È supportato un solo metodo di autenticazione alla volta.

Per ulteriori informazioni sull'attivazione dell'autenticazione basata su certificati, fare riferimento a. "Abilitare l'autenticazione sul backend dello storage ONTAP".

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Backend**.
2. Selezionare il backend dello storage.
3. Nel campo credenziali, selezionare l'icona **Modifica**.
4. Nella pagina Edit (Modifica), selezionare una delle seguenti opzioni.
   - **Usa credenziali amministratore**: Inserire l'indirizzo IP di gestione del cluster ONTAP e le credenziali di amministratore. Le credenziali devono essere credenziali a livello di cluster.

     L'utente di cui si inseriscono le credenziali deve disporre di `ontapi` Metodo di accesso all'accesso dell'utente abilitato in Gestione di sistema di ONTAP sul cluster ONTAP. Se si intende utilizzare la replica SnapMirror, applicare le credenziali utente con il ruolo "admin", che dispone dei metodi di accesso `ontapi` e. `http`, Sui cluster ONTAP di origine e di destinazione. Fare riferimento a. "Gestire gli account utente nella documentazione di ONTAP" per ulteriori informazioni.

   - **Usa un certificato**: Carica il certificato `.pem` file, la chiave del certificato `.key` e, facoltativamente, il file dell'autorità di certificazione.
5. Selezionare **Salva**.

Gestire un backend di storage rilevato

È possibile scegliere di gestire un backend di storage non gestito ma rilevato. Quando si gestisce un backend di storage, Astra Control indica se un certificato per l'autenticazione è scaduto.

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Backend**.
2. Selezionare l'opzione **rilevato**.
3. Selezionare il backend dello storage.
4. Dal menu Opzioni nella colonna **azioni**, selezionare **Gestisci**.
5. Apportare le modifiche.
6. Selezionare **Salva**.

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 il backend dello storage.
3. Dal menu Opzioni nella colonna **azioni**, selezionare **Annulla gestione**.
4. Digitare "unManage" per confermare l'azione.
5. Selezionare **Sì, Annulla gestione del backend di storage**.

Rimuovere un backend di storage

È possibile rimuovere un backend di storage non più in uso. Questa operazione può essere utile per mantenere la configurazione semplice e aggiornata.

Prima di iniziare

- Assicurarsi che il backend dello storage non sia gestito.
- Assicurarsi che il backend dello storage non abbia volumi associati al cluster.

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Backend**.
2. Se il backend viene gestito, annullarne la gestione.
   a. Selezionare **Managed**.
   b. Selezionare il backend dello storage.
   c. Dall'opzione **azioni**, selezionare **Annulla gestione**.
   d. Digitare "unManage" per confermare l'azione.
   e. Selezionare **Sì, Annulla gestione del backend di storage**.
3. Selezionare **rilevato**.
   a. Selezionare il backend dello storage.
   b. Dall'opzione **azioni**, selezionare **Rimuovi**.
   c. Digitare "remove" per confermare l'azione.
   d. Selezionare **Sì, rimuovere il backend di storage**.

Trova ulteriori informazioni

- "Utilizzare l'API di controllo Astra"

Monitorare le attività in esecuzione

In Astra Control è possibile visualizzare i dettagli relativi alle attività in esecuzione e alle attività che sono state completate, non riuscite o annullate nelle ultime 24 ore. Ad esempio, è possibile visualizzare lo stato di un'operazione di backup, ripristino o clonazione in esecuzione e visualizzare dettagli come percentuale completata e tempo rimanente stimato. È possibile visualizzare lo stato di un'operazione pianificata eseguita o avviata manualmente.

Durante la visualizzazione di un'attività in esecuzione o completata, è possibile espandere i dettagli dell'attività per visualizzare lo stato di ciascuna delle attività secondarie. La barra di avanzamento dell'attività è verde per le attività in corso o completate, blu per le attività annullate e rossa per le attività non riuscite a causa di un errore.

Per le operazioni di cloni, le sottoattività dell'attività consistono in un'operazione di snapshot e un'operazione di ripristino dello snapshot.

Per ulteriori informazioni sulle attività non riuscite, fare riferimento a. "Monitorare l'attività dell'account".

Fasi

1. Mentre un'attività è in esecuzione, passare a **applicazioni**.
2. Selezionare il nome di un'applicazione dall'elenco.
3. Nei dettagli dell'applicazione, selezionare la scheda **Tasks**.

   È possibile visualizzare i dettagli delle attività correnti o passate e filtrare in base allo stato dell'attività.

Le attività vengono conservate nell'elenco **Tasks** per un massimo di 24 ore. È possibile configurare questo limite e altre impostazioni di monitoraggio attività utilizzando "API di controllo Astra".

Monitorare l'infrastruttura con connessioni Cloud Insights, Prometheus o Fluentd

È possibile configurare diverse impostazioni opzionali per migliorare l'esperienza di Astra Control Center. Per monitorare e ottenere informazioni sulla tua infrastruttura completa, crea una connessione a NetApp Cloud Insights, configura Prometheus o Aggiungi una connessione Fluentd.

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.

- Connettersi a Cloud Insights
- Connettiti a Prometheus
- Connettersi a Fluentd

Aggiungere un server proxy per le connessioni a Cloud Insights o al sito di supporto NetApp

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.

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.

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.

Quando Astra Control Center è associato a Cloud Insights, non utilizzare l'opzione **Modifica distribuzione** in Cloud Insights.

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

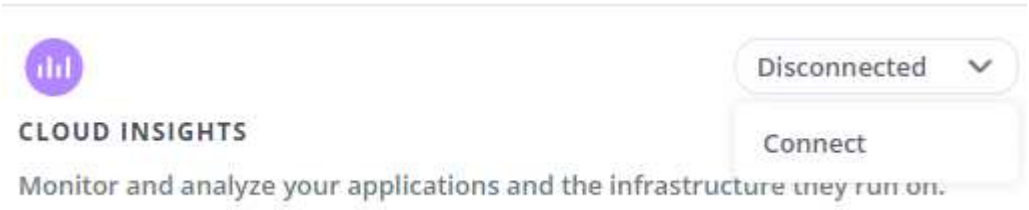
Prima di iniziare

- 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. Fare riferimento a. "Documentazione Cloud Insights".

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.



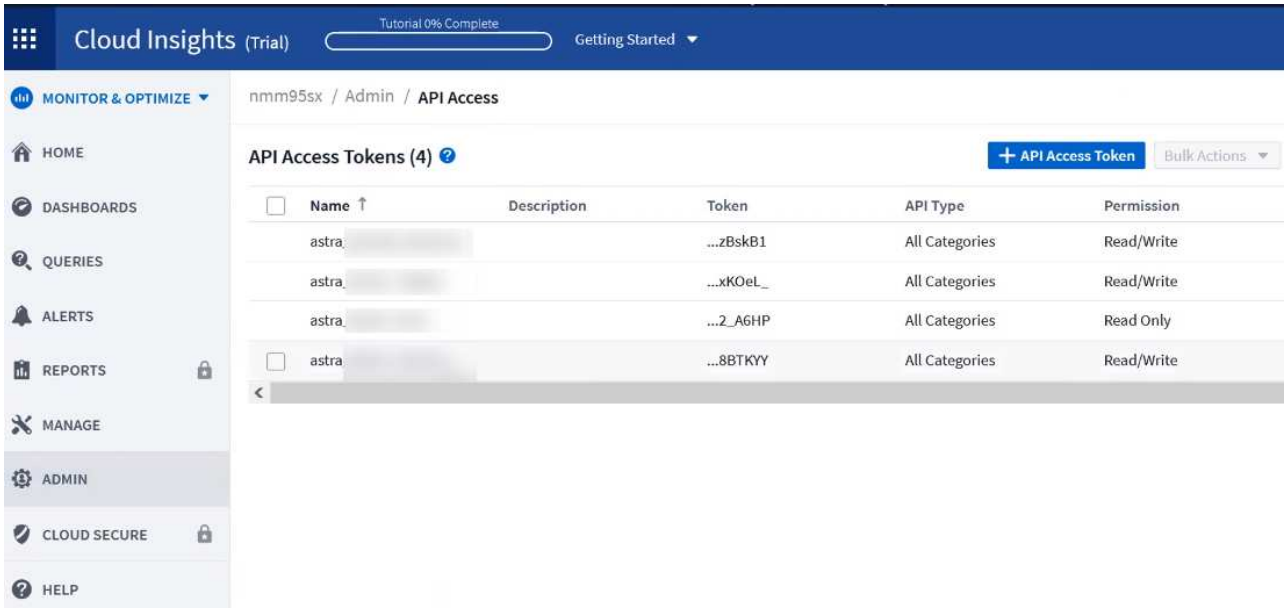
4. Inserire i token API Cloud Insights e l'URL del tenant. L'URL del tenant ha il seguente formato, ad esempio:

```
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 di accesso API **lettura/scrittura** e **sola lettura** facendo clic su **Amministratore** > **accesso API**.



c. Copiare la chiave **sola lettura**. Per attivare la connessione Cloud Insights, è necessario incollarla nella finestra di Astra Control Center. Per le autorizzazioni della chiave Read API Access Token, selezionare: Assets (risorse), Alerts (Avvisi), Acquisition Unit (unità di acquisizione) e Data Collection (raccolta dati).

d. Copiare la chiave **Read/Write**. È necessario incollarlo nella finestra di dialogo di Astra Control Center **Connect Cloud Insights**. Per le autorizzazioni della chiave del token di accesso API lettura/scrittura, selezionare: Acquisizione dati, acquisizione log, unità di acquisizione e raccolta dati.

> 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.

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

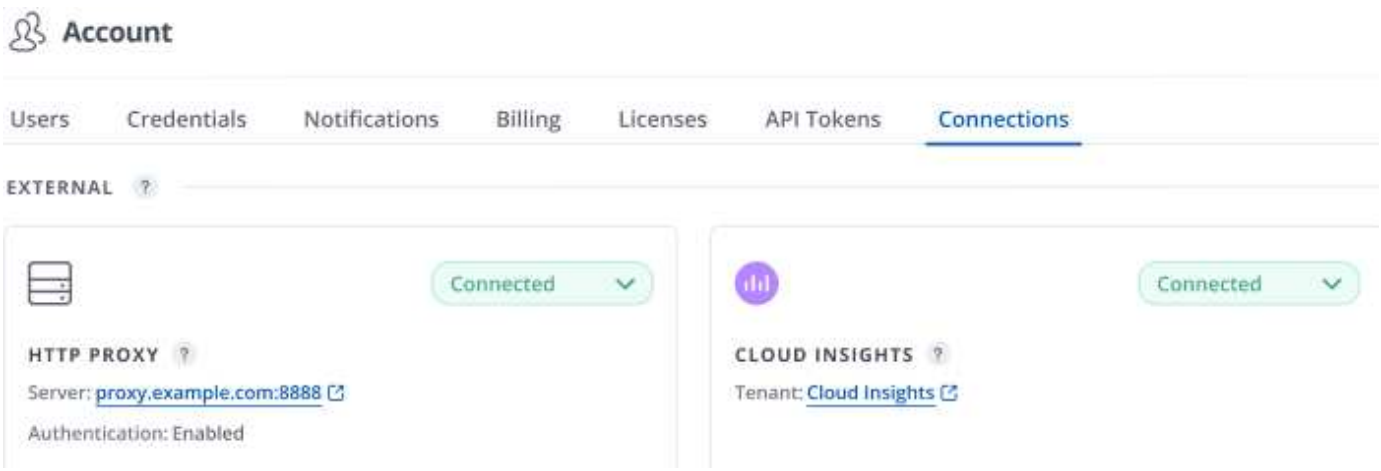
5. Selezionare **Connect**.

> 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.

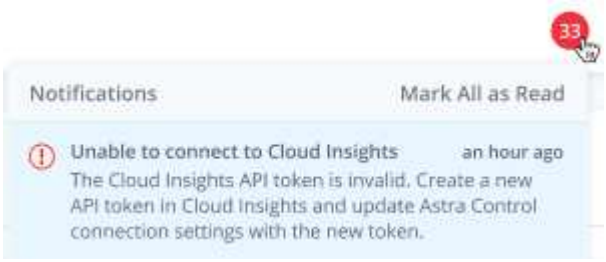
> Per passare facilmente da un'unità di controllo Astra a un'interfaccia utente Cloud Insights e viceversa, assicurarsi di aver effettuato l'accesso a entrambe.

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.

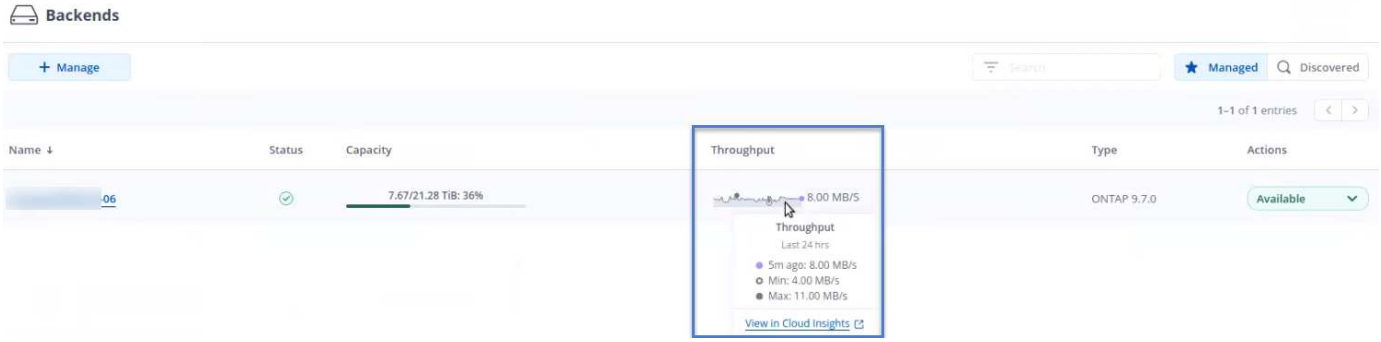


Se la connessione non è riuscita per qualche motivo, lo stato visualizza **Failed** (non riuscito). Il motivo del guasto è disponibile in **Notifiche** nella parte superiore destra dell'interfaccia utente.



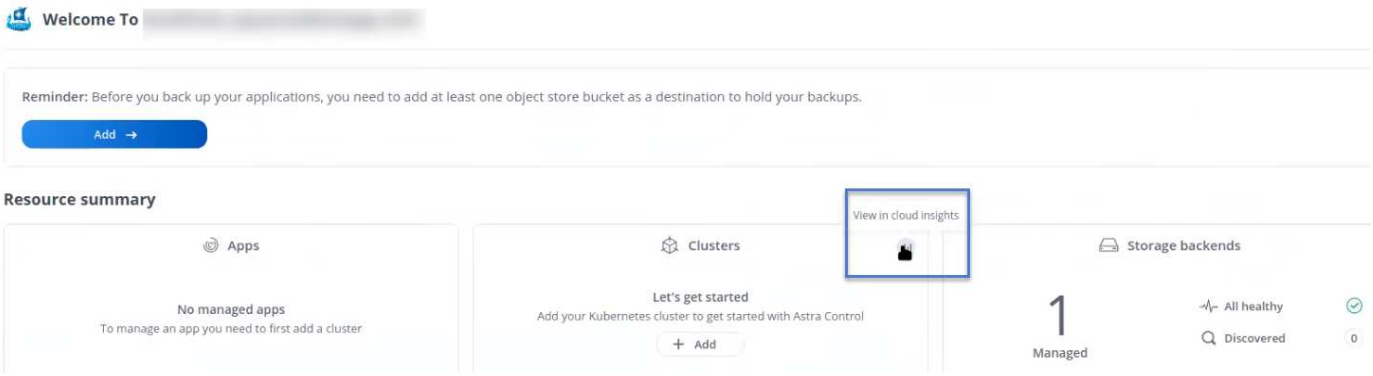
Le stesse informazioni sono disponibili anche in **account** > **Notifiche**.

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.



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.

Connettiti a Prometheus

Con Prometheus è possibile monitorare i dati di Astra Control Center. Puoi configurare Prometheus per raccogliere le metriche dall'endpoint di metriche del cluster Kubernetes e utilizzare Prometheus anche per visualizzare i dati delle metriche.

Per ulteriori informazioni sull'utilizzo di Prometheus, consultare la relativa documentazione all'indirizzo "Introduzione a Prometheus".

Di cosa hai bisogno

Assicurarsi di aver scaricato e installato il pacchetto Prometheus sul cluster Astra Control Center o su un cluster diverso in grado di comunicare con il cluster Astra Control Center.

Seguire le istruzioni nella documentazione ufficiale per "Installare Prometheus".

Prometheus deve essere in grado di comunicare con il cluster Astra Control Center Kubernetes. Se Prometheus non è installato sul cluster Astra Control Center, è necessario assicurarsi che sia in grado di comunicare con il servizio di metriche in esecuzione sul cluster Astra Control Center.

Configurare Prometheus

Astra Control Center espone un servizio di metriche sulla porta TCP 9090 nel cluster Kubernetes. Devi configurare Prometheus per raccogliere le metriche da questo servizio.

Fasi

1. Accedere al server Prometheus.
2. Aggiungere la voce del cluster in `prometheus.yml` file. In `yml` aggiungere una voce simile alla seguente per il cluster in `scrape_configs section`:

```
job_name: '<Add your cluster name here. You can abbreviate. It just
needs to be a unique name>'
  metrics_path: /accounts/<replace with your account ID>/metrics
  authorization:
     credentials: <replace with your API token>
  tls_config:
     insecure_skip_verify: true
  static_configs:
    - targets: ['<replace with your astraAddress. If using FQDN, the
prometheus server has to be able to resolve it>']
```

> Se si imposta `tls_config insecure_skip_verify` a. `true`, Il protocollo di crittografia TLS non è richiesto.

3. Riavviare il servizio Prometheus:

```
sudo systemctl restart prometheus
```

Accedi a Prometheus

Accedere all'URL Prometheus.

Fasi

1. In un browser, inserire l'URL Prometheus con la porta 9090.

2. Verificare la connessione selezionando **Status** > **Targets**.

Visualizza i dati in Prometheus

Puoi utilizzare Prometheus per visualizzare i dati di Astra Control Center.

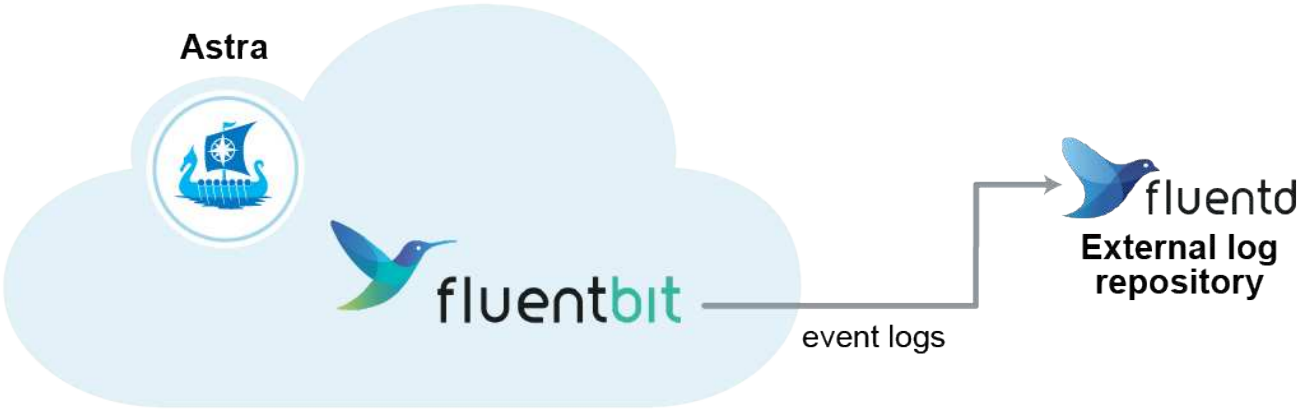
Fasi

1. In un browser, inserire l'URL Prometheus.
2. Dal menu Prometheus, selezionare **grafico**.
3. Per utilizzare Metrics Explorer (Esplora metriche), selezionare l'icona accanto a **Execute** (Esegui).
4. Selezionare `scrape_samples_scraped` E selezionare **Esegui**.
5. Per visualizzare lo scraping dei campioni nel tempo, selezionare **Graph** (grafico).

Se sono stati raccolti più dati del cluster, le metriche di ciascun cluster appaiono in un colore diverso.

Connettersi a Fluentd

È possibile inviare registri (eventi Kubernetes) da un sistema monitorato 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.

Prima di iniziare

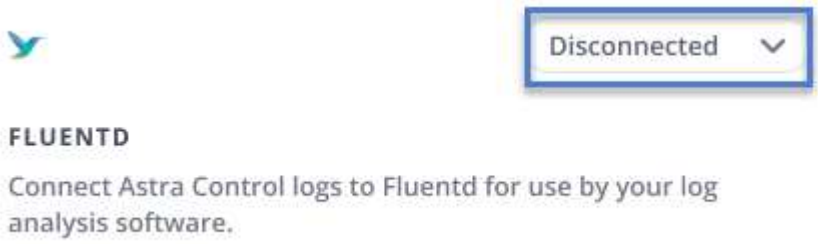
- Un account Astra Control Center con privilegi **admin**/**owner**.
- Astra Control Center installato e in esecuzione su un cluster Kubernetes.

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.



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.

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.

Quando si annulla la gestione di un'applicazione:

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

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **applicazioni**.
2. Selezionare l'applicazione.
3. Dal menu Opzioni nella colonna azioni, selezionare **UnGestisci**.
4. Esaminare le informazioni.
5. Digitare "unManage" per confermare.
6. Selezionare **Sì, Annulla gestione applicazione**.

Risultato

Astra Control Center interrompe la gestione dell'applicazione.

Annullare la gestione di un cluster

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

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

Quando si annulla la gestione di un cluster:

- 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.
- Astra Trident non verrà disinstallato dal cluster. "Scopri come disinstallare Astra Trident".

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Clusters**.
2. Selezionare la casella di controllo del cluster che non si desidera più gestire.
3. Dal menu Opzioni nella colonna **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). In seguito, il cluster verrà rimosso dalla pagina **Clusters** e non sarà 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.

Aggiornare Astra Control Center

Per aggiornare Astra Control Center, scaricare il pacchetto di installazione dal NetApp Support Site e completare queste istruzioni. È possibile utilizzare questa procedura per aggiornare Astra Control Center in ambienti connessi a Internet o con connessione ad aria.

Queste istruzioni descrivono il processo di upgrade per Astra Control Center dalla seconda release più recente a questa release corrente. Non è possibile eseguire l'aggiornamento direttamente da una versione che è costituita da due o più versioni precedenti alla release corrente. Se la versione installata di Astra Control Center è più recente, potrebbe essere necessario eseguire gli aggiornamenti della catena alle versioni più recenti fino a quando Astra Control Center installato non è solo una versione precedente alla versione più recente. Per un elenco completo delle versioni rilasciate, vedere "note di rilascio".

Prima di iniziare

Prima di eseguire l'aggiornamento, assicurarsi che l'ambiente soddisfi ancora "Requisiti minimi per l'implementazione di Astra Control Center". L'ambiente deve avere i seguenti requisiti:

- **A "supportato" Versione Astra Trident**

  Espandere per i passaggi

  Determinare la versione di Trident in esecuzione:

  ```
  kubectl get tridentversion -n trident
  ```

  Aggiornare Astra Trident, se necessario, utilizzando questi elementi "istruzioni".

La release 23,10 è l'ultima release di Astra Control Center che supporterà Astra Trident. Si consiglia vivamente di farlo "Abilita Astra Control Provisioner" Per accedere a funzionalità avanzate di gestione e provisioning dello storage oltre a quelle offerte da Astra Trident. È necessario eseguire l'aggiornamento ad Astra Control Center 23,10 e abilitare Astra Control Provivisioner per utilizzare questa funzionalità estesa. Astra Control Provisioner non funzionerà con le versioni precedenti di Astra Control Center.

- **Una distribuzione Kubernetes supportata**

Espandere per i passaggi

Determinare la versione di Kubernetes in esecuzione:

```
kubectl get nodes -o wide
```

- **Risorse cluster sufficienti**

Espandere per i passaggi

Determinare le risorse del cluster disponibili:

```
kubectl describe node <node name>
```

- **Un registro che è possibile utilizzare per inviare e caricare le immagini di Astra Control Center**
- **Una classe di archiviazione predefinita**

Espandere per i passaggi

Determinare la classe di storage predefinita:

```
kubectl get storageclass
```

- **Servizi API sani e disponibili**

Espandere per i passaggi

Assicurarsi che tutti i servizi API siano in buono stato e disponibili:

```
kubectl get apiservices
```

- **(solo OpenShift) operatori cluster sani e disponibili**

Espandere per i passaggi

Assicurarsi che tutti gli operatori del cluster siano in buono stato e disponibili.

```
kubectl get clusteroperators
```

- **Accedere al Registro di sistema dell'immagine di controllo Astra di NetApp**:

È possibile ottenere le immagini di installazione e i miglioramenti delle funzionalità per Astra Control, come Astra Control provisioner, dal registro delle immagini di NetApp.

Espandere per i passaggi

a. Registrare l'ID dell'account Astra Control necessario per accedere al Registro di sistema.

   Puoi visualizzare l'ID dell'account nell'interfaccia utente Web di Astra Control Service. Selezionare l'icona a forma di figura in alto a destra nella pagina, selezionare **accesso API** e annotare l'ID account.

b. Nella stessa pagina, selezionare **generate API token**, copiare la stringa del token API negli Appunti e salvarla nell'editor.

c. Accedere al registro Astra Control:

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

A proposito di questa attività

Il processo di aggiornamento di Astra Control Center ti guida attraverso le seguenti fasi di alto livello:

Disconnettersi dall'interfaccia utente di Astra Control Center prima di iniziare l'aggiornamento.

- Scarica ed estrai Astra Control Center
- Rimuovere il plug-in NetApp Astra kubectl e installarlo di nuovo
- Aggiungere le immagini al registro locale
- Installare l'operatore Astra Control Center aggiornato
- Aggiornare Astra Control Center
- Verificare lo stato del sistema

Non eliminare l'operatore di Astra Control Center (ad esempio, `kubectl delete -f astra_control_center_operator_deploy.yaml`) In qualsiasi momento durante l'aggiornamento o l'operazione di Astra Control Center per evitare di eliminare i pod.

Eseguire gli aggiornamenti in una finestra di manutenzione quando pianificazioni, backup e snapshot non sono in esecuzione.

Scarica ed estrai Astra Control Center

Puoi scegliere di scaricare il bundle Astra Control Center dal sito di supporto di NetApp o utilizzare Docker per estrarre il bundle dal registro delle immagini di Astra Control Service.

Sito di supporto NetApp

1. Scarica il bundle contenente Astra Control Center (`astra-control-center-[version].tar.gz`) da "Pagina di download di Astra Control Center".
2. (Consigliato ma opzionale) Scarica il bundle di certificati e firme per Astra Control Center (`astra-control-center-certs-[version].tar.gz`) per verificare la firma del bundle.

   Espandere per i dettagli

   ```
   tar -vxzf astra-control-center-certs-[version].tar.gz
   ```

   ```
   openssl dgst -sha256 -verify certs/AstraControlCenter-public.pub
   -signature certs/astra-control-center-[version].tar.gz.sig
   astra-control-center-[version].tar.gz
   ```

   Viene visualizzato l'output `Verified OK` una volta completata la verifica.

3. Estrarre le immagini dal bundle Astra Control Center:

   ```
   tar -vxzf astra-control-center-[version].tar.gz
   ```

Registro delle immagini di Astra Control

1. Effettua l'accesso ad Astra Control Service.
2. Nella Dashboard, selezionare **distribuire un'istanza autogestita di Astra Control**.
3. Seguire le istruzioni per accedere al registro delle immagini di Astra Control, estrarre l'immagine di installazione di Astra Control Center ed estrarre l'immagine.

Rimuovere il plug-in NetApp Astra kubectl e installarlo di nuovo

È possibile utilizzare il plug-in della riga di comando di NetApp Astra kubectl per inviare immagini a un repository Docker locale.

1. Determinare se il plug-in è installato:

   ```
   kubectl astra
   ```

2. Eseguire una delle seguenti operazioni:
   - Se il plugin è installato, il comando dovrebbe restituire il plugin kubectl help ed è possibile rimuovere la versione esistente di kubectl-astra: `delete /usr/local/bin/kubectl-astra`.
   - Se il comando restituisce un errore, il plug-in non è installato ed è possibile procedere con la fase successiva per installarlo.

3. Installare il plug-in:

   a. Elencare i binari del plugin NetApp Astra kubectl disponibili e annotare il nome del file necessario per il sistema operativo e l'architettura della CPU:

      La libreria di plugin kubectl fa parte del bundle tar e viene estratta nella cartella `kubectl-astra`.

```
ls kubectl-astra/
```

   a. Spostare il binario corretto nel percorso corrente e rinominarlo `kubectl-astra`:

```
cp kubectl-astra/<binary-name> /usr/local/bin/kubectl-astra
```

Aggiungere le immagini al registro locale

1. Completare la sequenza di passaggi appropriata per il motore dei container:

Docker

1. Passare alla directory root del tarball. Viene visualizzata la `acc.manifest.bundle.yaml` file e queste directory:

   ```
   acc/
   kubectl-astra/
   acc.manifest.bundle.yaml
   ```

2. Trasferire le immagini del pacchetto nella directory delle immagini di Astra Control Center nel registro locale. Eseguire le seguenti sostituzioni prima di eseguire `push-images` comando:

   - Sostituire <BUNDLE_FILE> con il nome del file bundle di controllo Astra (`acc.manifest.bundle.yaml`).
   - Sostituire <MY_FULL_REGISTRY_PATH> con l’URL del repository Docker; ad esempio, "<a href="https://<docker-registry>"" class="bare">https://<docker-registry>".
   - Sostituire <MY_REGISTRY_USER> con il nome utente.
   - Sostituire <MY_REGISTRY_TOKEN> con un token autorizzato per il registro.

   ```
   kubectl astra packages push-images -m <BUNDLE_FILE> -r
   <MY_FULL_REGISTRY_PATH> -u <MY_REGISTRY_USER> -p
   <MY_REGISTRY_TOKEN>
   ```

Podman

1. Passare alla directory root del tarball. Vengono visualizzati il file e la directory seguenti:

   ```
   acc/
   kubectl-astra/
   acc.manifest.bundle.yaml
   ```

2. Accedere al Registro di sistema:

   ```
   podman login <YOUR_REGISTRY>
   ```

3. Preparare ed eseguire uno dei seguenti script personalizzato per la versione di Podman utilizzata. Sostituire <MY_FULL_REGISTRY_PATH> con l'URL del repository che include le sottodirectory.

   ```
   <strong>Podman 4</strong>
   ```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.10.0-68
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done
```

```
<strong>Podman 3</strong>
```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.10.0-68
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done
```

Il percorso dell'immagine creato dallo script deve essere simile al seguente, a seconda della configurazione del Registro di sistema:

```
https://downloads.example.io/docker-astra-control-
prod/netapp/astra/acc/23.10.0-68/image:version
```

Installare l'operatore Astra Control Center aggiornato

1. Modificare la directory:

```
cd manifests
```

2. Modificare l'yaml di implementazione dell'operatore di Astra Control Center (`astra_control_center_operator_deploy.yaml`) per fare riferimento al registro locale e al segreto.

```
vim astra_control_center_operator_deploy.yaml
```

   a. Se si utilizza un registro che richiede l'autenticazione, sostituire o modificare la riga predefinita di `imagePullSecrets: []` con i seguenti elementi:

```
imagePullSecrets: [{name: astra-registry-cred}]
```

   b. Cambiare `ASTRA_IMAGE_REGISTRY` per `kube-rbac-proxy` al percorso del registro in cui sono state inviate le immagini in a. passaggio precedente.

   c. Cambiare `ASTRA_IMAGE_REGISTRY` per `acc-operator` al percorso del registro in cui sono state inviate le immagini in a. passaggio precedente.

   d. Aggiungere i seguenti valori a `env` sezione:

```
- name: ACCOP_HELM_UPGRADETIMEOUT
  value: 300m
```

Esempio astra_control_center_operator_deploy.yaml:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
  name: acc-operator-controller-manager
  namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
  strategy:
    type: Recreate
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
      containers:
      - args:
        - --secure-listen-address=0.0.0.0:8443
        - --upstream=http://127.0.0.1:8080/
        - --logtostderr=true
        - --v=10
        image: ASTRA_IMAGE_REGISTRY/kube-rbac-proxy:v4.8.0
        name: kube-rbac-proxy
        ports:
        - containerPort: 8443
          name: https
      - args:
        - --health-probe-bind-address=:8081
        - --metrics-bind-address=127.0.0.1:8080
        - --leader-elect
        env:
        - name: ACCOP_LOG_LEVEL
          value: "2"
        - name: ACCOP_HELM_UPGRADETIMEOUT
          value: 300m
        image: ASTRA_IMAGE_REGISTRY/acc-operator:23.10.72
        imagePullPolicy: IfNotPresent
        livenessProbe:
          httpGet:
            path: /healthz
```

```
            port: 8081
          initialDelaySeconds: 15
          periodSeconds: 20
        name: manager
        readinessProbe:
          httpGet:
            path: /readyz
            port: 8081
          initialDelaySeconds: 5
          periodSeconds: 10
        resources:
          limits:
            cpu: 300m
            memory: 750Mi
          requests:
            cpu: 100m
            memory: 75Mi
        securityContext:
          allowPrivilegeEscalation: false
      imagePullSecrets: []
      securityContext:
        runAsUser: 65532
      terminationGracePeriodSeconds: 10
```

3. Installare l'operatore Astra Control Center aggiornato:

```
kubectl apply -f astra_control_center_operator_deploy.yaml
```

Esempio di risposta:

```
namespace/netapp-acc-operator unchanged
customresourcedefinition.apiextensions.k8s.io/astracontrolcenters.as
tra.netapp.io configured
role.rbac.authorization.k8s.io/acc-operator-leader-election-role
unchanged
clusterrole.rbac.authorization.k8s.io/acc-operator-manager-role
configured
clusterrole.rbac.authorization.k8s.io/acc-operator-metrics-reader
unchanged
clusterrole.rbac.authorization.k8s.io/acc-operator-proxy-role
unchanged
rolebinding.rbac.authorization.k8s.io/acc-operator-leader-election-
rolebinding unchanged
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-manager-
rolebinding configured
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-proxy-
rolebinding unchanged
configmap/acc-operator-manager-config unchanged
service/acc-operator-controller-manager-metrics-service unchanged
deployment.apps/acc-operator-controller-manager configured
```

4. Verificare che i pod siano in esecuzione:

```
kubectl get pods -n netapp-acc-operator
```

Aggiornare Astra Control Center

1. Modificare la risorsa personalizzata Astra Control Center (CR):

```
kubectl edit AstraControlCenter -n [netapp-acc or custom namespace]
```

2. Modificare il numero di versione di Astra (`astraVersion` all'interno di `spec`) da `23.07.0` a. `23.10.0`:

> Non è possibile eseguire l'aggiornamento direttamente da una versione che è costituita da due o più versioni precedenti alla release corrente. Per un elenco completo delle versioni rilasciate, vedere "note di rilascio".

```
spec:
  accountName: "Example"
  astraVersion: "[Version number]"
```

3. Verificare che il percorso del Registro di sistema dell'immagine corrisponda al percorso del Registro di sistema in cui sono state inviate le immagini in passaggio precedente. Aggiornare `imageRegistry` all'interno di `spec` se il registro di sistema è stato modificato dall'ultima installazione.

```
  imageRegistry:
    name: "[your_registry_path]"
```

4. Aggiungere quanto segue al `crds` configurazione all'interno di `spec`:

```
crds:
  shouldUpgrade: true
```

5. Aggiungere le seguenti righe all'interno di `additionalValues` all'interno di `spec` In Astra Control Center CR:

```
additionalValues:
    nautilus:
      startupProbe:
        periodSeconds: 30
        failureThreshold: 600
    keycloak-operator:
      livenessProbe:
        initialDelaySeconds: 180
      readinessProbe:
        initialDelaySeconds: 180
```

6. Salvare e uscire dall'editor di file. Le modifiche verranno applicate e l'aggiornamento avrà inizio.
7. (Facoltativo) verificare che i pod terminino e diventino nuovamente disponibili:

```
watch kubectl get pods -n [netapp-acc or custom namespace]
```

8. Attendere che le condizioni di stato di Astra Control indichino che l'aggiornamento è completo e pronto (`True`):

```
kubectl get AstraControlCenter -n [netapp-acc or custom namespace]
```

Risposta:

```
NAME    UUID                                   VERSION     ADDRESS
READY
astra   9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f   23.10.0-68
10.111.111.111  True
```

Per monitorare lo stato dell'aggiornamento durante l'operazione, eseguire il seguente comando: `kubectl get AstraControlCenter -o yaml -n [netapp-acc or custom namespace]`

Per esaminare i registri dell'operatore di Astra Control Center, eseguire il seguente comando:
`kubectl logs deploy/acc-operator-controller-manager -n netapp-acc-operator -c manager -f`

Verificare lo stato del sistema

1. Accedere ad Astra Control Center.
2. Verificare che la versione sia stata aggiornata. Consultare la pagina **supporto** nell'interfaccia utente.
3. Verificare che tutti i cluster e le applicazioni gestiti siano ancora presenti e protetti.

Abilita Astra Control Provisioner

Astra Trident le versioni 23,10 e successive includono la possibilità di utilizzare Astra Control Provivisioner, che consente agli utenti dotati di licenza Astra Control di accedere a funzionalità avanzate di provisioning dello storage. Astra Control Provisioner fornisce questa funzionalità estesa oltre alle funzionalità standard basate su CSI Astra Trident.

In arrivo gli update di Astra Control, Astra Control Provivisioner sostituirà Astra Trident come provisioner di storage e orchestrator nell'architettura Astra Control. Per questo motivo, si consiglia vivamente agli utenti di Astra Control di attivare Astra Control Provisioner. Astra Trident continuerà a rimanere open source e ad essere rilasciato, mantenuto, supportato e aggiornato con le nuove CSI e altre funzionalità di NetApp.

A proposito di questa attività

È necessario seguire questa procedura se si è un utente di Astra Control Center con licenza e si sta cercando di utilizzare la funzionalità di Astra Control Provisioner. Devi seguire questa procedura anche se sei un utente di Astra Trident e desideri utilizzare le funzionalità aggiuntive fornite da Astra Control Provisioner senza utilizzare Astra Control.

Per ogni caso, la funzionalità di provisioning non è abilitata per impostazione predefinita in Astra Trident 23,10, ma può essere abilitata utilizzando questo processo.

Prima di iniziare

Se stai abilitando Astra Control provisioner, esegui prima quanto segue:

Utenti di Astra Control Provisioners con Astra Control Center

- **Ottenere una licenza Astra Control Center**: È necessario un "Licenza Astra Control Center" Per abilitare Astra Control Provisioner e accedere alle funzionalità fornite.
- **Installa o esegui l'aggiornamento ad Astra Control Center 23,10**: Avrai bisogno di questa versione se hai intenzione di utilizzare Astra Control Provisioner con Astra Control.
- **Confirmi che il tuo cluster ha un'architettura di sistema AMD64**: L'immagine Astra Control Provivisioner è fornita in entrambe le architetture CPU AMD64 e ARM64, ma solo AMD64 è supportato da Astra Control Center.
- **Ottenere un account del Servizio di controllo Astra per l'accesso al Registro di sistema**: Se si intende utilizzare il Registro di sistema di controllo Astra piuttosto che il Sito di supporto NetApp per scaricare l'immagine del revisioner di controllo Astra, completare la registrazione per un "Account Astra Control Service". Dopo aver completato e inviato il modulo e creato un account BlueXP, riceverai un'email di benvenuto con Astra Control Service.
- **Se Astra Trident è installato, conferma che la sua versione si trovi all'interno di una finestra a quattro release**: Puoi eseguire un aggiornamento diretto a Astra Trident 23,10 con Astra Control Provisioner se il tuo Astra Trident si trova all'interno di una finestra a quattro release della versione 23,10. Ad esempio, puoi eseguire l'upgrade direttamente da Astra Trident 22,10 a 23,10.

Solo utenti di Astra Control provisioner

- **Ottenere una licenza Astra Control Center**: È necessario un "Licenza Astra Control Center" Per abilitare Astra Control Provisioner e accedere alle funzionalità fornite.
- **Se Astra Trident è installato, conferma che la sua versione si trovi all'interno di una finestra a quattro release**: Puoi eseguire un aggiornamento diretto a Astra Trident 23,10 con Astra Control Provisioner se il tuo Astra Trident si trova all'interno di una finestra a quattro release della versione 23,10. Ad esempio, puoi eseguire l'upgrade direttamente da Astra Trident 22,10 a 23,10.
- **Prendi un account Astra Control Service per l'accesso al Registro di sistema**: Per scaricare le immagini di Astra Control provisioner, è necessario accedere al Registro di sistema. Per iniziare, completa la registrazione per un "Account Astra Control Service". Dopo aver completato e inviato il modulo e creato un account BlueXP, riceverai un'email di benvenuto con Astra Control Service.

(Fase 1) scaricare ed estrarre Astra Control Provisioner

Gli utenti di Astra Control Center possono scaricare l'immagine usando il metodo del registro di sistema o il sito di supporto di NetApp. Gli utenti di Astra Trident che desiderano utilizzare Astra Control Protivisioner senza Astra Control devono utilizzare il metodo del Registro di sistema.

(Opzionale) Sito di supporto NetApp

1. Scarica il bundle Astra Control Provisioner (`trident-acp-[version].tar`) da "Pagina di download di Astra Control Center".
2. (Consigliato ma facoltativo) scaricate il pacchetto di certificati e firme per Astra Control Center (astra-control-center-certs-[version].tar.gz) per verificare la firma del pacchetto trident-acp-[version] tar.

Espandere per i dettagli

```
tar -vxzf astra-control-center-certs-[version].tar.gz
```

```
openssl dgst -sha256 -verify certs/AstraControlCenterDockerImages-public.pub -signature certs/trident-acp-[version].tar.sig trident-acp-[version].tar
```

3. Caricare l'immagine di Astra Control provisioner:

```
docker load < trident-acp-23.10.0.tar
```

Risposta:

```
Loaded image: trident-acp:23.10.0-linux-amd64
```

4. Contrassegnare l'immagine:

```
docker tag trident-acp:23.10.0-linux-amd64 <my_custom_registry>/trident-acp:23.10.0
```

5. Inviare l'immagine al registro personalizzato:

```
docker push <my_custom_registry>/trident-acp:23.10.0
```

(Opzione) Registro di sistema delle immagini Astra Control

È possibile utilizzare Podman invece di Docker per i comandi di questa procedura. Se si utilizza un ambiente Windows, si consiglia di utilizzare PowerShell.

1. Accedere al Registro di sistema dell'immagine di controllo Astra di NetApp:
   a. Accedere all'interfaccia utente Web di Astra Control Service e selezionare l'icona raffigurata in alto a destra nella pagina.
   b. Selezionare **API access**.
   c. Annotare l'ID account.
   d. Nella stessa pagina, selezionare **generate API token**, copiare la stringa del token API negli Appunti e salvarla nell'editor.
   e. Accedere al registro Astra Control utilizzando il metodo preferito:

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

```
crane auth login cr.astra.netapp.io -u <account-id> -p <api-token>
```

2. Se si dispone di un Registro di sistema personalizzato, attenersi alla procedura descritta di seguito per spostare l'immagine nel Registro di sistema personalizzato. Se non si utilizza un registro, seguire i passaggi dell'operatore Trident nel "sezione successiva".

> Per i seguenti comandi, puoi utilizzare Podman al posto di Docker. Se si utilizza un ambiente Windows, si consiglia di utilizzare PowerShell.

Docker

a. Estrarre l'immagine di Astra Control provisioner dal Registro di sistema:

> L'immagine estratta non supporta più piattaforme e supporta solo la stessa piattaforma dell'host che ha estratto l'immagine, ad esempio Linux AMD64.

```
docker pull cr.astra.netapp.io/astra/trident-acp:23.10.0
--platform <cluster platform>
```

Esempio:

```
docker pull cr.astra.netapp.io/astra/trident-acp:23.10.0
--platform linux/amd64
```

b. Contrassegnare l'immagine:

```
docker tag cr.astra.netapp.io/astra/trident-acp:23.10.0
<my_custom_registry>/trident-acp:23.10.0
```

c. Inviare l'immagine al registro personalizzato:

```
docker push <my_custom_registry>/trident-acp:23.10.0
```

Gru

a. Copiare il manifesto di Astra Control Provisioner nel registro personalizzato:

```
crane copy cr.astra.netapp.io/astra/trident-acp:23.10.0
<my_custom_registry>/trident-acp:23.10.0
```

(Fase 2) attiva Astra Control Provisioner in Astra Trident

Determinare se il metodo di installazione originale ha utilizzato un e completare i passaggi appropriati in base al metodo originale.

> Non utilizzare Helm per abilitare Astra Control Provisioner. Se hai utilizzato Helm per l'installazione originale e stai effettuando l'aggiornamento a 23,10, dovrai utilizzare l'operatore Trident o tridentctl per eseguire l'abilitazione di Astra Control Provisioner.

Operatore Astra Trident

1. "Scaricare il programma di installazione di Astra Trident ed estrarlo".
2. Completa questi passaggi se non hai ancora installato Astra Trident o se hai rimosso l'operatore dall'implementazione originale di Astra Trident:
   a. Creare il CRD:

```
kubectl create -f
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.16.y
aml
```

   b. Creare lo spazio dei nomi tridente (`kubectl create namespace trident`) o confermare che lo spazio dei nomi tridente esiste ancora (`kubectl get all -n trident`). Se lo spazio dei nomi è stato rimosso, crearlo di nuovo.
3. Aggiorna Astra Trident alla versione 23.10.0:

> Per i cluster che eseguono Kubernetes 1.24 o versioni precedenti, utilizzare `bundle_pre_1_25.yaml`. Per i cluster che eseguono Kubernetes 1.25 o versioni successive, utilizzare `bundle_post_1_25.yaml`.

```
kubectl -n trident apply -f trident-installer-
23.10.0/deploy/<bundle-name.yaml>
```

4. Verificare che Astra Trident sia in esecuzione:

```
kubectl get torc -n trident
```

   Risposta:

```
NAME      AGE
trident   21m
```

5. se si dispone di un registro che utilizza segreti, creare un segreto da utilizzare per estrarre l'immagine di Astra Control Provisioner:

```
kubectl create secret docker-registry <secret_name> -n trident
--docker-server=<my_custom_registry> --docker-username=<username>
--docker-password=<token>
```

6. Modificare il TridentOrchestrator CR e apportare le seguenti modifiche:

```
kubectl edit torc trident -n trident
```

a. Impostare una posizione del Registro di sistema personalizzata per l'immagine Astra Trident o estrarla dal Registro di sistema Astra Control (`tridentImage: <my_custom_registry>/trident:23.10.0` oppure `tridentImage: netapp/trident:23.10.0`).

b. Abilita Astra Control Provisioner (`enableACP: true`).

c. Impostare la posizione del Registro di sistema personalizzata per l'immagine Astra Control Provivioner o estrarla dal Registro di sistema Astra Control (`acpImage: <my_custom_registry>/trident-acp:23.10.0` oppure `acpImage: cr.astra.netapp.io/astra/trident-acp:23.10.0`).

d. Se stabilito segreti di estrazione delle immagini in precedenza, è possibile impostarle qui (`imagePullSecrets: - <secret_name>`). Usare lo stesso nome segreto che hai stabilito nei passaggi precedenti.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  tridentImage: <registry>/trident:23.10.0
  enableACP: true
  acpImage: <registry>/trident-acp:23.10.0
  imagePullSecrets:
  - <secret_name>
```

7. Salvare e uscire dal file. Il processo di distribuzione si avvia automaticamente.
8. Verificare che l'operatore, la distribuzione e i replicaset siano stati creati.

```
kubectl get all -n trident
```

> In un cluster Kubernetes dovrebbe esserci solo **un'istanza** dell'operatore. Non creare implementazioni multiple dell'operatore Astra Trident.

9. Verificare `trident-acp` il container è in esecuzione e così `acpVersion` è `23.10.0` con stato di `Installed`:

```
kubectl get torc -o yaml
```

Risposta:

```
status:
  acpVersion: 23.10.0
  currentInstallationParams:
    ...
    acpImage: <registry>/trident-acp:23.10.0
    enableACP: "true"
    ...
  ...
  status: Installed
```

tridentctl

1. "Scaricare il programma di installazione di Astra Trident ed estrarlo".
2. "Se disponi già di un Astra Trident, disinstallarlo dal cluster che lo ospita".
3. Installa Astra Trident con Astra Control Provisioner abilitato (`--enable-acp=true`):

```
./tridentctl -n trident install --enable-acp=true --acp
-image=mycustomregistry/trident-acp:23.10
```

4. Confermare che Astra Control Provisioner è stato abilitato:

```
./tridentctl -n trident version
```

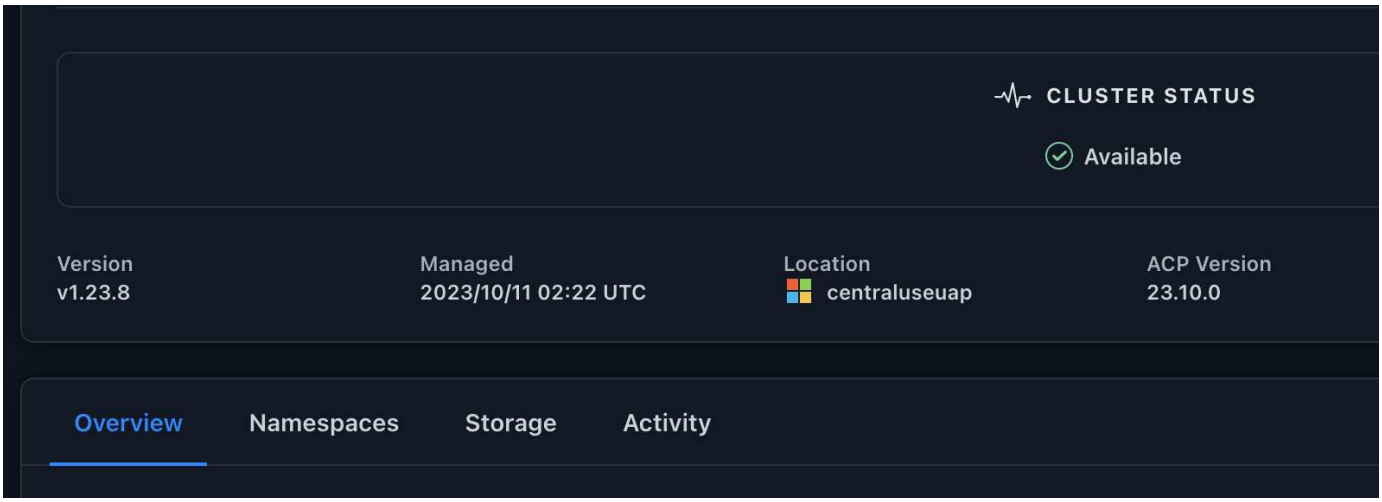
Risposta:

```
+----------------+----------------+-------------+ | SERVER VERSION |
CLIENT VERSION | ACP VERSION | +----------------+----------------
+-------------+ | 23.10.0 | 23.10.0 | 23.10.0. | +----------------
+----------------+-------------+
```

Risultato

La funzionalità Astra Control Provisioner è abilitata ed è possibile utilizzare qualsiasi funzionalità disponibile per la versione in esecuzione.

(Solo per gli utenti di Astra Control Center) dopo l'installazione di Astra Control provisioner, il cluster che ospita il provisioner nell'interfaccia utente di Astra Control Center mostrerà un `ACP version` piuttosto che `Trident version` campo e numero della versione installata corrente.



Per ulteriori informazioni

- "Documentazione sugli aggiornamenti di Astra Trident"

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.

In caso di problemi con la disinstallazione, vedere Risoluzione dei problemi di disinstallazione.

Prima di iniziare

1. "Annulla gestione di tutte le applicazioni" sui cluster.
2. "Annulla gestione di tutti i 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.yaml -n netapp-acc
   ```

   Risultato:

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

2. Utilizzare il seguente comando per eliminare `netapp-acc` namespace (o personalizzato):

   ```
   kubectl delete ns [netapp-acc or custom namespace]
   ```

   Risultato di esempio:

```
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
```

Risoluzione dei problemi di disinstallazione

Utilizzare le seguenti soluzioni alternative per risolvere eventuali problemi riscontrati durante la disinstallazione di Astra Control Center.

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

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

Fasi

1. Eliminare `acc-monitoring` agente:

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

Risultato:

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

2. Eliminare lo spazio dei nomi:

```
kubectl delete ns netapp-monitoring
```

Risultato:

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

3. Conferma la rimozione delle risorse:

```
kubectl get pods -n netapp-monitoring
```

Risultato:

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

4. Conferma rimozione dell'agente di monitoraggio:

```
kubectl get crd|grep agent
```

Risultato del campione:

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

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

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

Risultato:

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

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

È possibile eliminare manualmente i CRD Traefik. Le CRDS sono risorse globali e l'eliminazione di queste risorse potrebbe avere un impatto sulle altre applicazioni del cluster.

Fasi

1. Elencare i CRD Traefik installati sul cluster:

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

   Risposta

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

2. Eliminare i CRD:

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

Trova ulteriori informazioni

- "Problemi noti per la disinstallazione"

Utilizza Astra Control Provisioner

Configurare la crittografia backend dello storage

Con Astra Control Provivisioner, puoi migliorare la sicurezza dell'accesso ai dati abilitando la crittografia per il traffico tra il cluster gestito e il backend dello storage.

Astra Control Provivisioner supporta la crittografia Kerberos per due tipi di backend di storage:

- **On-Premise ONTAP** - Astra Control Protivisioner supporta la crittografia Kerberos su connessioni NFSv3 e NFSv4 da Red Hat OpenShift e dai cluster Kubernetes upstream ai volumi ONTAP on-premise.
- **Azure NetApp Files** - Astra Control Provisioner supporta la crittografia Kerberos su connessioni NFSv4,1 da cluster Kubernetes upstream a volumi Azure NetApp Files.

Puoi creare, eliminare, ridimensionare, creare snapshot, clonare clone di sola lettura e importare i volumi che utilizzano la crittografia NFS.

Configura la crittografia Kerberos in-flight con i volumi ONTAP in sede

È possibile abilitare la crittografia Kerberos sul traffico di storage tra il cluster gestito e un backend di storage ONTAP on-premise.

> La crittografia Kerberos per il traffico NFS con backend di storage ONTAP in sede è supportata solo utilizzando `ontap-nas` driver di storage.

Prima di iniziare

- Assicurati di aver abilitato Astra Control Provisioner nel cluster gestito. Fare riferimento a. "Abilita Astra Control Provisioner" per istruzioni.
- Assicurarsi di avere accesso a. `tridentctl` utility.
- Assicurarsi di disporre dell'accesso come amministratore al back-end dello storage ONTAP.
- Conoscere il nome del volume o dei volumi che si desidera condividere dal back-end dello storage ONTAP.
- Verificare di aver preparato la VM di storage ONTAP per supportare la crittografia Kerberos per i volumi NFS. Fare riferimento a. "Attivare Kerberos su una LIF dati" per istruzioni.
- Verificare che tutti i volumi NFSv4 utilizzati con la crittografia Kerberos siano configurati correttamente. Consultare la sezione Configurazione di dominio NetApp NFSv4 (pagina 13) della "Guida ai miglioramenti e alle Best practice di NetApp NFSv4".

Aggiungere o modificare criteri di esportazione ONTAP

Devi aggiungere regole alle policy di esportazione ONTAP esistenti o creare nuove policy di esportazione che supportino la crittografia Kerberos per il volume root delle macchine virtuali di storage ONTAP, oltre a qualsiasi volume ONTAP condiviso con il cluster Kubernetes upstream. Le regole dei criteri di esportazione aggiunte o i nuovi criteri di esportazione creati devono supportare i seguenti protocolli di accesso e autorizzazioni di accesso:

Protocolli di accesso

Configura la policy di esportazione con i protocolli di accesso NFS, NFSv3 e NFSv4.

Dettagli di accesso

È possibile configurare una delle tre diverse versioni della crittografia Kerberos, a seconda delle esigenze del volume:

- **Kerberos 5** - (autenticazione e crittografia)
- **Kerberos 5i** - (autenticazione e crittografia con protezione dell'identità)
- **Kerberos 5p** - (autenticazione e crittografia con protezione di identità e privacy)

Configurare la regola dei criteri di esportazione ONTAP con le autorizzazioni di accesso appropriate. Ad esempio, se i cluster montano i volumi NFS con una combinazione di crittografia Kerberos 5i e Kerberos 5p, utilizza le seguenti impostazioni di accesso:

Tipo	Accesso in sola lettura	Accesso in lettura/scrittura	Accesso superutente
UNIX	Attivato	Attivato	Attivato
Kerberos 5i	Attivato	Attivato	Attivato
Kerberos 5p	Attivato	Attivato	Attivato

Per informazioni su come creare policy di esportazione e regole delle policy di esportazione di ONTAP, consulta la seguente documentazione:

- "Creare una policy di esportazione"
- "Aggiungere una regola a un criterio di esportazione"

Creazione di un backend dello storage

Puoi creare una configurazione backend dello storage Astra Control Provivisioner che include funzionalità di crittografia Kerberos.

A proposito di questa attività

Quando si crea un file di configurazione backend di archiviazione che configura la crittografia Kerberos, è possibile specificare una delle tre versioni diverse della crittografia Kerberos utilizzando `spec.nfsMountOptions` parametro:

- `spec.nfsMountOptions: sec=krb5` (autenticazione e crittografia)
- `spec.nfsMountOptions: sec=krb5i` (autenticazione e crittografia con protezione dell'identità)
- `spec.nfsMountOptions: sec=krb5p` (autenticazione e crittografia con protezione di identità e privacy)

Specificare un solo livello Kerberos. Se si specificano più livelli di crittografia Kerberos nell'elenco dei parametri, viene utilizzata solo la prima opzione.

Fasi

1. Nel cluster gestito, creare un file di configurazione backend dello storage utilizzando l'esempio seguente. Sostituire i valori tra parentesi <> con le informazioni dell'ambiente:

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-ontap-nas-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-ontap-nas
spec:
  version: 1
  storageDriverName: "ontap-nas"
  managementLIF: <STORAGE_VM_MGMT_LIF_IP_ADDRESS>
  dataLIF: <PROTOCOL_LIF_FQDN_OR_IP_ADDRESS>
  svm: <STORAGE_VM_NAME>
  username: <STORAGE_VM_USERNAME_CREDENTIAL>
  password: <STORAGE_VM_PASSWORD_CREDENTIAL>
  nasType: nfs
  nfsMountOptions: ["sec=krb5i"] #can be krb5, krb5i, or krb5p
  qtreesPerFlexvol:
  credentials:
    name: backend-ontap-nas-secret
```

2. Utilizzare il file di configurazione creato nel passaggio precedente per creare il backend:

```
tridentctl create backend -f <backend-configuration-file>
```

Se la creazione del backend non riesce, si è verificato un errore nella configurazione del backend. È possibile visualizzare i log per determinare la causa eseguendo il seguente comando:

```
tridentctl logs
```

Dopo aver identificato e corretto il problema con il file di configurazione, è possibile eseguire nuovamente il comando create.

Creare una classe di storage

È possibile creare una classe di archiviazione per il provisioning dei volumi con la crittografia Kerberos.

A proposito di questa attività

Quando si crea un oggetto classe di archiviazione, è possibile specificare una delle tre versioni diverse della crittografia Kerberos utilizzando `mountOptions` parametro:

- `mountOptions: sec=krb5` (autenticazione e crittografia)
- `mountOptions: sec=krb5i` (autenticazione e crittografia con protezione dell'identità)
- `mountOptions: sec=krb5p` (autenticazione e crittografia con protezione di identità e privacy)

Specificare un solo livello Kerberos. Se si specificano più livelli di crittografia Kerberos nell'elenco dei parametri, viene utilizzata solo la prima opzione. Se il livello di crittografia specificato nella configurazione backend di archiviazione è diverso dal livello specificato nell'oggetto della classe di archiviazione, l'oggetto della classe di archiviazione ha la precedenza.

Fasi

1. Creare un oggetto Kubernetes StorageClass, usando il seguente esempio:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nas-sc
provisioner: csi.trident.netapp.io
mountOptions: ["sec=krb5i"] #can be krb5, krb5i, or krb5p
parameters:
  backendType: "ontap-nas"
  storagePools: "ontapnas_pool"
  trident.netapp.io/nasType: "nfs"
allowVolumeExpansion: True
```

2. Creare la classe di storage:

```
kubectl create -f sample-input/storage-class-ontap-nas-sc.yaml
```

3. Assicurarsi che la classe di archiviazione sia stata creata:

```
kubectl get sc ontap-nas-sc
```

   L'output dovrebbe essere simile a quanto segue:

```
NAME          PROVISIONER             AGE
ontap-nas-sc    csi.trident.netapp.io   15h
```

Provisioning dei volumi

Dopo aver creato un backend di storage e una classe di storage, è ora possibile eseguire il provisioning di un

volume. Per istruzioni, fare riferimento a. "Provisioning di un volume".

Configurare la crittografia Kerberos in-flight con i volumi Azure NetApp Files

È possibile attivare la crittografia Kerberos sul traffico di storage tra il cluster gestito e un singolo backend di storage Azure NetApp Files o un pool virtuale di backend di storage Azure NetApp Files.

Prima di iniziare

- Assicurati di aver abilitato Astra Control Provivisioner sul cluster Red Hat OpenShift gestito. Fare riferimento a. "Abilita Astra Control Provisioner" per istruzioni.
- Assicurarsi di avere accesso a. `tridentctl` utility.
- Assicurarsi di aver preparato il backend dello storage Azure NetApp Files per la crittografia Kerberos annotando i requisiti e seguendo le istruzioni in "Documentazione Azure NetApp Files".
- Verificare che tutti i volumi NFSv4 utilizzati con la crittografia Kerberos siano configurati correttamente. Consultare la sezione Configurazione di dominio NetApp NFSv4 (pagina 13) della "Guida ai miglioramenti e alle Best practice di NetApp NFSv4".

Creazione di un backend dello storage

È possibile creare una configurazione backend dello storage Azure NetApp Files che include la funzionalità di crittografia Kerberos.

A proposito di questa attività

Quando si crea un file di configurazione backend dello storage che configura la crittografia Kerberos, è possibile definirlo in modo che venga applicato a uno dei due livelli possibili:

- Il **livello backend di archiviazione** utilizzando `spec.kerberos` campo
- Il livello **pool virtuale** utilizzando `spec.storage.kerberos` campo

Quando si definisce la configurazione a livello del pool virtuale, il pool viene selezionato utilizzando l'etichetta nella classe di archiviazione.

In entrambi i livelli, è possibile specificare una delle tre diverse versioni della crittografia Kerberos:

- `kerberos: sec=krb5` (autenticazione e crittografia)
- `kerberos: sec=krb5i` (autenticazione e crittografia con protezione dell'identità)
- `kerberos: sec=krb5p` (autenticazione e crittografia con protezione di identità e privacy)

Fasi

1. Nel cluster gestito, creare un file di configurazione backend dello storage utilizzando uno dei seguenti esempi, a seconda del punto in cui occorre definire il backend dello storage (livello di backend dello storage o livello del pool virtuale). Sostituire i valori tra parentesi <> con le informazioni dell'ambiente:

Esempio di livello di backend di archiviazione

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-anf-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-anf-secret
```

Esempio di livello del pool virtuale

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-anf-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  storage:
    - labels:
        type: encryption
      kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-anf-secret
```

2. Utilizzare il file di configurazione creato nel passaggio precedente per creare il backend:

```
tridentctl create backend -f <backend-configuration-file>
```

Se la creazione del backend non riesce, si è verificato un errore nella configurazione del backend. È possibile visualizzare i log per determinare la causa eseguendo il seguente comando:

```
tridentctl logs
```

Dopo aver identificato e corretto il problema con il file di configurazione, è possibile eseguire nuovamente il comando create.

Creare una classe di storage

È possibile creare una classe di archiviazione per il provisioning dei volumi con la crittografia Kerberos.

Fasi

1. Creare un oggetto Kubernetes StorageClass, usando il seguente esempio:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: anf-sc-nfs
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "nfs"
  selector: "type=encryption"
```

2. Creare la classe di storage:

```
kubectl create -f sample-input/storage-class-anf-sc-nfs.yaml
```

3. Assicurarsi che la classe di archiviazione sia stata creata:

```
kubectl get sc anf-sc-nfs
```

L'output dovrebbe essere simile a quanto segue:

```
NAME          PROVISIONER             AGE
anf-sc-nfs    csi.trident.netapp.io   15h
```

Provisioning dei volumi

Dopo aver creato un backend di storage e una classe di storage, è ora possibile eseguire il provisioning di un volume. Per istruzioni, fare riferimento a. "Provisioning di un volume".

Ripristina i dati dei volumi utilizzando uno snapshot

Astra Control Provivisioner esegue un ripristino rapido e in-place dei volumi da uno snapshot utilizzando `TridentActionSnapshotRestore` (TASR) CR. Questo CR funziona come un'azione imperativa di Kubernetes e non persiste al termine

dell'operazione.

Astra Control provisioner supporta il ripristino delle snapshot su `ontap-san`, `ontap-san-economy`, `ontap-nas`, `ontap-nas-flexgroup`, `azure-netapp-files`, `gcp-cvs`, e. `solidfire-san` driver.

Prima di iniziare

È necessario disporre di un PVC associato e di uno snapshot del volume disponibile.

- Verificare che lo stato del PVC sia limitato.

```
kubectl get pvc
```

- Verificare che lo snapshot del volume sia pronto per l'uso.

```
kubectl get vs
```

Fasi

1. Creare TASR CR. In questo esempio viene creato un CR per PVC `pvc1` e snapshot del volume `pvc1-snapshot`.

```
cat tasr-pvc1-snapshot.yaml

apiVersion: trident.netapp.io/v1
kind: TridentActionSnapshotRestore
metadata:
  name: this-doesnt-matter
  namespace: trident
spec:
  pvcName: pvc1
  volumeSnapshotName: pvc1-snapshot
```

2. Applicare la CR per eseguire il ripristino dall'istantanea. In questo esempio vengono ripristinati gli snapshot `pvc1`.

```
kubectl create -f tasr-pvc1-snapshot.yaml

tridentactionsnapshotrestore.trident.netapp.io/this-doesnt-matter
created
```

Risultati

Astra Control Provivisioner ripristina i dati dalla snapshot. È possibile verificare lo stato di ripristino dello snapshot.

```
kubectl get tasr -o yaml

apiVersion: trident.netapp.io/v1
items:
- apiVersion: trident.netapp.io/v1
  kind: TridentActionSnapshotRestore
  metadata:
    creationTimestamp: "2023-04-14T00:20:33Z"
    generation: 3
    name: this-doesnt-matter
    namespace: trident
    resourceVersion: "3453847"
    uid: <uid>
  spec:
    pvcName: pvc1
    volumeSnapshotName: pvc1-snapshot
  status:
    startTime: "2023-04-14T00:20:34Z"
    completionTime: "2023-04-14T00:20:37Z"
    state: Succeeded
kind: List
metadata:
  resourceVersion: ""
```

- Nella maggior parte dei casi, Astra Control provisioner non ritenta automaticamente l'operazione in caso di guasto. Sarà necessario eseguire nuovamente l'operazione.
- Gli utenti Kubernetes senza accesso amministrativo potrebbero dover essere autorizzati dall'amministratore a creare una TASR CR nel namespace delle applicazioni.

Replica dei volumi con SnapMirror

Con Astra Control Provivisioner, puoi creare relazioni di mirroring tra un volume di origine su un cluster e il volume di destinazione sul cluster in peering per replicare i dati per il disaster recovery. È possibile utilizzare una definizione di risorsa personalizzata (CRD) con nome per eseguire le seguenti operazioni:

- Creare relazioni di mirroring tra volumi (PVC)
- Rimuovere le relazioni di mirroring tra volumi
- Interrompere le relazioni di mirroring
- Promozione del volume secondario in condizioni di disastro (failover)
- Eseguire la transizione senza perdita di dati delle applicazioni da cluster a cluster (durante failover o migrazioni pianificati)

Prerequisiti per la replica

Prima di iniziare, verificare che siano soddisfatti i seguenti prerequisiti:

Cluster ONTAP

- **Astra Control Provisioner**: Astra Control Provisioner versione 22,10 o successiva deve esistere sia sui cluster Kubernetes di origine che di destinazione che utilizzano ONTAP come backend.
- **Licenze**: Le licenze asincrone di ONTAP SnapMirror che utilizzano il bundle di protezione dati devono essere attivate sia sul cluster ONTAP di origine che su quello di destinazione. Fare riferimento a. "Panoramica sulle licenze SnapMirror in ONTAP" per ulteriori informazioni.

Peering

- **Cluster e SVM**: I backend dello storage ONTAP devono essere peering. Fare riferimento a. "Panoramica del peering di cluster e SVM" per ulteriori informazioni.

  Assicurati che i nomi delle SVM utilizzati nella relazione di replica tra due cluster ONTAP siano univoci.

- **Astra Control Provisioner e SVM**: Le SVM remote in cui è stato eseguito il peering devono essere disponibili per Astra Control Provisioner nel cluster di destinazione.

Driver supportati

- La replica di un volume è supportata per i driver ontap-nas e ontap-san.

Creare un PVC specchiato

Seguire questi passaggi e utilizzare gli esempi CRD per creare una relazione di mirroring tra volumi primari e secondari.

Fasi

1. Eseguire i seguenti passaggi sul cluster Kubernetes primario:
   a. Creare un oggetto StorageClass con `trident.netapp.io/replication: true` parametro.

      Esempio

      ```
      apiVersion: storage.k8s.io/v1
      kind: StorageClass
      metadata:
        name: csi-nas
      provisioner: csi.trident.netapp.io
      parameters:
        backendType: "ontap-nas"
        fsType: "nfs"
        trident.netapp.io/replication: "true"
      ```

   b. Crea un PVC con StorageClass creato in precedenza.

Esempio

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: csi-nas
spec:
  accessModes:
  - ReadWriteMany
  resources:
    requests:
      storage: 1Gi
  storageClassName: csi-nas
```

c. Creare una CR MirrorRelationship con informazioni locali.

Esempio

```
kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
spec:
  state: promoted
  volumeMappings:
  - localPVCName: csi-nas
```

Astra Control Provivisioner recupera le informazioni interne del volume e dello stato attuale di data Protection (DP) del volume, quindi popola il campo di stato di MirrorRelationship.

d. Procurarsi il TridentMirrorRelationship CR per ottenere il nome interno e la SVM del PVC.

```
kubectl get tmr csi-nas
```

```
kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
  generation: 1
spec:
  state: promoted
  volumeMappings:
  - localPVCName: csi-nas
status:
  conditions:
  - state: promoted
    localVolumeHandle:
"datavserver:trident_pvc_3bedd23c_46a8_4384_b12b_3c38b313c1e1"
    localPVCName: csi-nas
    observedGeneration: 1
```

2. Eseguire i seguenti passaggi sul cluster Kubernetes secondario:
   a. Creare una classe StorageClass con il parametro trident.netapp.io/replication: true.

      Esempio

      ```
      apiVersion: storage.k8s.io/v1
      kind: StorageClass
      metadata:
        name: csi-nas
      provisioner: csi.trident.netapp.io
      parameters:
        trident.netapp.io/replication: true
      ```

   b. Creare una CR MirrorRelationship con informazioni sulla destinazione e sulla sorgente.

      Esempio

      ```
      kind: TridentMirrorRelationship
      apiVersion: trident.netapp.io/v1
      metadata:
        name: csi-nas
      spec:
        state: established
        volumeMappings:
        - localPVCName: csi-nas
          remoteVolumeHandle:
      "datavserver:trident_pvc_3bedd23c_46a8_4384_b12b_3c38b313c1e1"
      ```

Astra Control Provisioner creerà una relazione SnapMirror con il nome della policy di relazione configurata (o default per ONTAP) e la inizializzerà.

c. Crea un PVC con StorageClass creato in precedenza per agire come secondario (destinazione SnapMirror).

Esempio

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: csi-nas
  annotations:
    trident.netapp.io/mirrorRelationship: csi-nas
spec:
  accessModes:
  - ReadWriteMany
resources:
  requests:
    storage: 1Gi
storageClassName: csi-nas
```

Astra Control Provisioner controllerà la CRD TridentMirrorRelationship e non creerà il volume se la relazione non esiste. Se esiste una relazione, Astra Control Provisioner garantirà che il nuovo volume FlexVol venga inserito in una SVM a cui viene inviata la SVM remota definita in MirrorRelationship.

Stati di replica dei volumi

Una relazione mirror Trident (TMR) è un CRD che rappresenta un'estremità di una relazione di replica tra PVC. Il TMR di destinazione ha uno stato, che indica ad Astra Control Provisioner lo stato desiderato. Il TMR di destinazione ha i seguenti stati:

- **Stabilito**: Il PVC locale è il volume di destinazione di una relazione speculare, e questa è una nuova relazione.
- **Promosso**: Il PVC locale è ReadWrite e montabile, senza alcuna relazione speculare attualmente in vigore.
- **Ristabilito**: Il PVC locale è il volume di destinazione di una relazione speculare ed era anche precedentemente in quella relazione speculare.
  - Lo stato ristabilito deve essere utilizzato se il volume di destinazione era in una relazione con il volume di origine perché sovrascrive il contenuto del volume di destinazione.
  - Se il volume non era precedentemente in relazione con l'origine, lo stato ristabilito non riuscirà.

Promozione del PVC secondario durante un failover non pianificato

Eseguire il seguente passaggio sul cluster Kubernetes secondario:

- Aggiornare il campo *spec.state* di TridentMirrorRelationship su `promoted`.

Promozione del PVC secondario durante un failover pianificato

Durante un failover pianificato (migrazione), eseguire le seguenti operazioni per promuovere il PVC secondario:

Fasi

1. Sul cluster Kubernetes primario, creare una snapshot del PVC e attendere la creazione dello snapshot.
2. Sul cluster Kubernetes primario, creare SnapshotInfo CR per ottenere dettagli interni.

   Esempio

   ```
   kind: SnapshotInfo
   apiVersion: trident.netapp.io/v1
   metadata:
     name: csi-nas
   spec:
     snapshot-name: csi-nas-snapshot
   ```

3. Nel cluster Kubernetes secondario, aggiornare il campo *spec.state* del *TridentMirrorRelationship* CR a *Promoted* e *spec.promotedSnapshotHandle* come nome interno dello snapshot.
4. Sul cluster Kubernetes secondario, confermare lo stato (campo status.state) di TridentMirrorRelationship a promosso.

Ripristinare una relazione di mirroring dopo un failover

Prima di ripristinare una relazione di specchiatura, scegliere il lato che si desidera creare come nuovo primario.

Fasi

1. Nel cluster Kubernetes secondario, verificare che i valori per il campo *spec.remoteVolumeHandle* in TridentMirrorRelationship siano aggiornati.
2. Sul cluster Kubernetes secondario, aggiornare il campo *spec.mirror* di TridentMirrorRelationship a. `reestablished`.

Operazioni supplementari

Astra Control Provivisioner supporta le seguenti operazioni sui volumi primario e secondario:

Replicare il PVC primario in un nuovo PVC secondario

Assicurarsi di disporre già di un PVC primario e di un PVC secondario.

Fasi

1. Eliminare i CRD PersistentVolumeClaim e TridentMirrorRelationship dal cluster (destinazione) secondario stabilito.
2. Eliminare il CRD TridentMirrorRelationship dal cluster primario (origine).
3. Creare un nuovo CRD TridentMirrorRelationship nel cluster primario (di origine) per il nuovo PVC secondario (di destinazione) che si desidera stabilire.

Ridimensionare un PVC specchiato, primario o secondario

Il PVC può essere ridimensionato normalmente, ONTAP espanderà automaticamente qualsiasi flevxols di destinazione se la quantità di dati supera le dimensioni correnti.

Rimuovere la replica da un PVC

Per rimuovere la replica, eseguire una delle seguenti operazioni sul volume secondario corrente:

- Eliminare MirrorRelationship sul PVC secondario. Questo interrompe la relazione di replica.
- In alternativa, aggiornare il campo spec.state a *Promoted*.

Eliminazione di un PVC (precedentemente specchiato)

Astra Control Provivisioner verifica la presenza di PVC replicati e rilascia la relazione di replica prima di tentare di eliminare il volume.

Eliminare una TMR

L'eliminazione di una TMR su un lato di una relazione specchiata fa sì che la TMR rimanente passi allo stato *promosso* prima che Astra Control Provivisioner completi l'eliminazione. Se il TMR selezionato per l'eliminazione è già nello stato *promosso*, non esiste alcuna relazione di mirror esistente e il TMR verrà rimosso e Astra Control Provisioner promuoverà il PVC locale in *ReadWrite*. Questa eliminazione rilascia i metadati SnapMirror per il volume locale in ONTAP. Se in futuro questo volume viene utilizzato in una relazione di mirroring, deve utilizzare un nuovo TMR con uno stato di replica del volume *stabilito* quando si crea la nuova relazione di mirroring.

Aggiorna relazioni mirror quando ONTAP è online

Le relazioni speculari possono essere aggiornate in qualsiasi momento dopo che sono state stabilite. È possibile utilizzare `state: promoted` oppure `state: reestablished` per aggiornare le relazioni. Quando si trasferisce un volume di destinazione a un volume ReadWrite regolare, è possibile utilizzare *PromotedSnapshotHandle* per specificare uno snapshot specifico su cui ripristinare il volume corrente.

Aggiorna relazioni di mirroring quando ONTAP non è in linea

Puoi utilizzare un CRD per eseguire un update di SnapMirror senza che Astra Control disponga di connettività diretta al cluster ONTAP. Fare riferimento al seguente formato di esempio di TridentActionMirrorUpdate:

Esempio

```
apiVersion: trident.netapp.io/v1
kind: TridentActionMirrorUpdate
metadata:
  name: update-mirror-b
spec:
  snapshotHandle: "pvc-1234/snapshot-1234"
  tridentMirrorRelationshipName: mirror-b
```

`status.state` Riflette lo stato del CRD TridentActionMirrorUpdate. Può assumere un valore da *riuscito*, *in corso* o *non riuscito*.

Automatizza con l’API REST di Astra Control

Automazione mediante l’API REST di Astra Control

Astra Control dispone di un’API REST che consente di accedere direttamente alla funzionalità Astra Control utilizzando un linguaggio di programmazione o un’utility come Curl. Puoi anche gestire le implementazioni di Astra Control utilizzando Ansible e altre tecnologie di automazione.

Per configurare e gestire le applicazioni Kubernetes, è possibile utilizzare l’interfaccia utente di Astra Control Center o l’API di Astra Control.

Per ulteriori informazioni, visitare il sito "Documentazione di automazione Astra".

Conoscenza e supporto

Risoluzione dei problemi

Scopri come risolvere alcuni problemi comuni che potresti incontrare.

"Knowledge base NetApp per Astra Control"

Trova ulteriori informazioni

- "Come caricare un file su NetApp (accesso richiesto)"
- "Come caricare manualmente un file su NetApp (accesso richiesto)"

Richiedi assistenza

NetApp fornisce supporto per Astra Control in diversi modi. Sono disponibili numerose opzioni di supporto self-service gratuite 24 ore su 24, 7 giorni su 7, come articoli della knowledge base (KB) e un canale di discording. Il tuo account Astra Control include il supporto tecnico remoto via web ticketing.

> Se si dispone di una licenza di valutazione per Astra Control Center, è possibile ottenere supporto tecnico. Tuttavia, la creazione del caso tramite il NetApp Support Site (NSS) non è disponibile. Puoi contattare il supporto tramite l'opzione di feedback o utilizzare il canale di discordia per il self-service.

Devi prima "Attivare il supporto per il numero di serie NetApp" per utilizzare queste opzioni di supporto non self-service. È necessario un account SSO NetApp Support Site (NSS) per la chat e il web ticketing insieme alla gestione del caso.

Opzioni di supporto automatico

È possibile accedere alle opzioni di supporto dall'interfaccia utente di Astra Control Center selezionando la scheda **Support** (supporto) dal menu principale.

Queste opzioni sono disponibili gratuitamente, 24 ore su 24, 7 giorni su 7:

- **"Utilizzare la knowledge base** (è richiesto l'accesso)": Cerca articoli, FAQ o informazioni di riparazione in caso di interruzione relative ad Astra Control.
- **Fare riferimento alla documentazione del prodotto**: Questo è il sito della documentazione attualmente visualizzato.
- **"Richiedi assistenza tramite discordia"**: Vai ad Astra nella categoria Pub per entrare in contatto con colleghi ed esperti.
- **Creare un caso di supporto**: Generare pacchetti di supporto da fornire al supporto NetApp per la risoluzione dei problemi.
- **Invia un feedback su Astra Control**: Invia un'e-mail a astra.feedback@netapp.com per farci conoscere le tue opinioni, le tue idee o i tuoi dubbi.

Abilita il caricamento giornaliero del bundle di supporto pianificato sul supporto NetApp

Durante l'installazione di Astra Control Center, se specificato `enrolled: true` per `autoSupport` Nel file CR (Custom Resource) di Astra Control Center (`astra_control_center.yaml`), i pacchetti di supporto giornalieri vengono caricati automaticamente su "Sito di supporto NetApp".

Generare bundle di supporto da fornire al supporto NetApp

Astra Control Center consente all'utente amministratore di generare bundle, che includono informazioni utili al supporto NetApp, inclusi registri, eventi per tutti i componenti dell'implementazione Astra, metriche e informazioni sulla topologia dei cluster e delle applicazioni in gestione. Se si è connessi a Internet, è possibile caricare pacchetti di supporto sul NetApp Support Site (NSS) direttamente dall'interfaccia utente di Astra Control Center.

> Il tempo impiegato da Astra Control Center per generare il bundle dipende dalle dimensioni dell'installazione di Astra Control Center e dai parametri del bundle di supporto richiesto. La durata specificata per la richiesta di un bundle di supporto determina il tempo necessario per la generazione del bundle (ad esempio, un periodo di tempo più breve comporta una generazione più rapida del bundle).

Prima di iniziare

Determinare se sarà richiesta una connessione proxy per caricare bundle su NSS. Se è necessaria una connessione proxy, verificare che Astra Control Center sia stato configurato per l'utilizzo di un server proxy.

1. Selezionare **account** > **connessioni**.
2. Controllare le impostazioni del proxy in **Impostazioni di connessione**.

Fasi

1. Creare un caso sul portale NSS utilizzando il numero di serie della licenza elencato nella pagina **Support** dell'interfaccia utente di Astra Control Center.
2. Per generare il bundle di supporto, attenersi alla seguente procedura utilizzando l'interfaccia utente di Astra Control Center:
   a. Nella sezione Support bundle della pagina **Support**, selezionare **generate**.
   b. Nella finestra **generate a Support Bundle** (genera un pacchetto di supporto), selezionare il periodo di tempo.

      È possibile scegliere tra tempi rapidi o personalizzati.

      > È possibile scegliere un intervallo di date personalizzato e specificare un periodo di tempo personalizzato durante l'intervallo di date.

   c. Una volta effettuate le selezioni, selezionare **Confirm** (Conferma).
   d. Selezionare la casella di controllo **caricare il bundle nel sito di supporto NetApp quando generato**.
   e. Selezionare **generate Bundle** (genera bundle).

      Quando il bundle di supporto è pronto, viene visualizzata una notifica nella pagina **account** > **notifica** nell'area Avvisi, nella pagina **attività** e nell'elenco delle notifiche (accessibile selezionando l'icona nella parte superiore destra dell'interfaccia utente).

Se la generazione non riesce, viene visualizzata un'icona nella pagina generate Bundle (genera bundle). Selezionare l'icona per visualizzare il messaggio.

L'icona delle notifiche nella parte superiore destra dell'interfaccia utente fornisce informazioni sugli eventi correlati al bundle di supporto, ad esempio quando il bundle viene creato correttamente, quando la creazione del bundle non riesce, quando il bundle non può essere caricato, quando il bundle non può essere scaricato e così via.

Se si dispone di un'installazione con aria compressa

Se si dispone di un'installazione con aria compressa, attenersi alla seguente procedura dopo la generazione del pacchetto di supporto.
Quando il bundle è disponibile per il download, l'icona Download viene visualizzata accanto a **generate** nella sezione **Support Bundle** della pagina **Support**.

Fasi

1. Selezionare l'icona Download per scaricare il pacchetto localmente.
2. Caricare manualmente il bundle su NSS.

   A tale scopo, è possibile utilizzare uno dei seguenti metodi:

   - Utilizzare "NetApp Authenticated file Upload (accesso richiesto)".
   - Collegare il bundle alla custodia direttamente su NSS.
   - Utilizzare Digital Advisor.

Trova ulteriori informazioni

- "Come caricare un file su NetApp (accesso richiesto)"
- "Come caricare manualmente un file su NetApp (accesso richiesto)"

Versioni precedenti della documentazione di Astra Control Center

È disponibile la documentazione per le release precedenti.

- "Documentazione di Astra Control Center 23.04"
- "Documentazione di Astra Control Center 22.11"
- "Documentazione di Astra Control Center 22.08"
- "Documentazione di Astra Control Center 22.04"
- "Documentazione di Astra Control Center 21.12"
- "Documentazione di Astra Control Center 21.08"

Note legali

Le note legali forniscono l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

"https://www.netapp.com/company/legal/trademarks/"

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Direttiva sulla privacy

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

- "Avviso per Astra Control Center"

Licenza API Astra Control

https://docs.netapp.com/us-en/astra-automation/media/astra-api-license.pdf

Informazioni sul copyright

Informazioni sul marchio commerciale