



Gestire le applicazioni

Astra Control Center

NetApp
June 06, 2024

Sommario

- Gestire le applicazioni 1
 - Inizia a gestire le app 1
 - Definire un esempio di applicazione personalizzata 7

Gestire le applicazioni

Inizia a gestire le app

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

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 una licenza Astra Control Center.
- **Namespaces:** Astra Control richiede che un'applicazione non si estende più di un singolo namespace, ma uno spazio dei nomi può contenere più di un'applicazione.
- **StorageClass:** Se si installa un'applicazione con un StorageClass esplicitamente impostato e si deve clonare l'applicazione, il cluster di destinazione per l'operazione di clone deve avere la StorageClass originariamente specificata. Il cloning di un'applicazione con un StorageClass esplicitamente impostato su un cluster che non ha lo stesso StorageClass avrà esito negativo.
- **Kubernetes resources:** Le applicazioni che utilizzano Kubernetes Resources 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
 - CustomResourceDefinition
 - CustomResource
 - DaemonSet
 - Implementazione
 - DeploymentConfig
 - Ingresso
 - MutatingWebhook
 - PersistentVolumeClaim
 - Pod
 - ReplicaSet
 - RoleBinding
 - Ruolo
 - Percorso
 - Segreto
 - Servizio
 - 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. Questi operatori sono generalmente progettati con un'architettura "pass-by-value" piuttosto che "pass-by-reference". Di seguito sono riportate alcune applicazioni per operatori che seguono questi modelli:
 - ["Apache K8ssandra"](#)
 - ["Ci Jenkins"](#)
 - ["Cluster XtraDB Percona"](#)

Si noti che Astra Control potrebbe non essere in grado di clonare un operatore progettato con un'architettura "pass-by-reference" (ad esempio, l'operatore CockroachDB). Durante questi tipi di operazioni di cloning, l'operatore clonato tenta di fare riferimento ai segreti di Kubernetes dall'operatore di origine, nonostante abbia il proprio nuovo segreto come parte del processo di cloning. L'operazione di clonazione potrebbe non riuscire perché Astra Control non è a conoscenza dei segreti di Kubernetes nell'operatore di origine.



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 assicurarsi che questo sia il caso.

Installa le app sul tuo cluster

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

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

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

Gestire le applicazioni

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



Le applicazioni installate con Helm 2 non sono supportate.

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

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



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

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



Dopo un'operazione di protezione dei dati (clone, backup, ripristino) e il successivo ridimensionamento persistente del volume, si verifica un ritardo di venti minuti prima che le nuove dimensioni del volume vengano visualizzate nell'interfaccia utente. L'operazione di protezione dei dati viene eseguita correttamente in pochi minuti ed è possibile utilizzare il software di gestione per il back-end dello storage per confermare la modifica delle dimensioni del volume.

Gestire le applicazioni in base allo spazio dei nomi

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

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

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

Fasi

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

Name	Ready	Cluster	Group	Discovered	Actions
default	✓	sc...	grp_default	2021/06/28 17:36 UTC	Managed
default1	✓	sc...	grp1_default	2021/06/28 17:36 UTC	Unmanaged
default2	✓	sc...	grp2_default	2021/06/28 17:36 UTC	Unmanaged
netapp-acc-operator	✓	sc...	netapp-acc-operator	2021/07/13 12:36 UTC	Unmanaged
pcloud	✓	sc...	pcloud	2021/07/13 12:37 UTC	Unmanaged

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

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

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

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

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

Name	Ready	Protected	Cluster	Group	Discovered	Actions
apppt	✓	⚠	sc...	app-logging	2021/06/28 17:36 UTC	Available

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

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

Risultato

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

Gestisci le app in base all'etichetta Kubernetes

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

Fasi

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

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

Dopo aver scelto un'etichetta, questa viene visualizzata nel campo **etichetta**. Astra Control aggiorna anche la sezione **risorse non selezionate** per mostrare le risorse che non corrispondono all'etichetta selezionata.

f. **Risorse non selezionate**: Verifica le risorse dell'app che non desideri proteggere.

4. Selezionare **Definisci applicazione personalizzata**.

Risultato

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

Ignorare le applicazioni

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

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

Fasi

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

Annulla gestione delle applicazioni

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



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

Fasi

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

E le applicazioni di sistema?

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

Name	Ready	Cluster	Discovered	Actions
...	✓	se-...	2021/06/28 17:36 UTC	Managed
...	✓	se-...	2021/06/28 17:36 UTC	Unmanaged
...	✓	se-...	2021/06/28 17:36 UTC	Unmanaged
default	...	se-...	2021/07/22 18:22 UTC	Discovering

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



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

Trova ulteriori informazioni

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

Definire un esempio di applicazione personalizzata

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

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

- Clonare
- Snapshot
- Backup
- Policy di protezione

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

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

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



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

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



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

Esempio: Policy di protezione separata per la release canary

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

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

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

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

Fasi

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

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

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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

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

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

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

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

Informazioni sul marchio commerciale

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