



Monitoring des Applikations- und Cluster-Systemzustands

Astra Control Center

NetApp
November 21, 2023

Inhalt

- Monitoring des Applikations- und Cluster-Systemzustands 1
 - Zeigen Sie eine Zusammenfassung des Applikations- und Cluster-Zustands an 1
 - Zeigen Sie den Cluster-Zustand an und managen Sie Storage-Klassen 2
 - Anzeigen des Funktionszustands und der Details einer App 3

Monitoring des Applikations- und Cluster-Systemzustands

Zeigen Sie eine Zusammenfassung des Applikations- und Cluster-Zustands an

Wählen Sie das **Dashboard** aus, um eine übergeordnete Ansicht Ihrer Apps, Cluster, Storage-Back-Ends und deren Integrität anzuzeigen.

Dabei handelt es sich nicht nur um statische Zahlen oder Statusangaben, sondern Sie können von jedem einzelnen Detail aus darauf aufgehen. Wenn Apps beispielsweise nicht vollständig geschützt sind, können Sie mit dem Mauszeiger auf das Symbol zeigen, um zu ermitteln, welche Apps nicht vollständig geschützt sind. Dies gibt einen Grund dafür.

Auf Applikationen Kachel

Mit der Kachel *Applications* können Sie Folgendes identifizieren:

- Wie viele Applikationen managen Sie aktuell mit Astra?
- Ob diese verwalteten Apps gesund sind.
- Gibt an, ob die Applikationen vollständig gesichert sind (sie sind geschützt, wenn neueste Backups verfügbar sind).
- Die Anzahl der Anwendungen, die erkannt, aber noch nicht verwaltet wurden.

Idealerweise wäre diese Zahl null, da Sie Apps nach dem Entstehen verwalten oder ignorieren würden. Anschließend sollten Sie die Anzahl der im Dashboard ermittelten Apps überwachen, um zu ermitteln, wann Entwickler neue Apps zu einem Cluster hinzufügen.

Cluster-Tile

Die Kachel **Cluster** bietet ähnliche Details über die Integrität der Cluster, die Sie mit dem Astra Control Center verwalten, und Sie können detaillierte Informationen abrufen, wie Sie es mit einer App möglich sind.

Storage Back-Ends

Die Kachel **Storage Back-Ends** enthält Informationen, die Ihnen bei der Identifizierung des Zustands von Storage-Back-Ends helfen. Dazu gehören:

- Wie viele Storage-Back-Ends werden gemanagt
- Gibt an, ob diese gemanagten Backends gesund sind
- Gibt an, ob die Back-Ends vollständig geschützt sind
- Die Anzahl der Back-Ends, die zwar erkannt, aber noch nicht gemanagt werden.

Zeigen Sie den Cluster-Zustand an und managen Sie Storage-Klassen

Nachdem Sie Cluster hinzugefügt haben, die von Astra Control Center gemanagt werden können, können Sie Details zum Cluster anzeigen, beispielsweise den Speicherort, die Worker-Nodes, die persistenten Volumes und die Storage-Klassen. Sie können auch die Standard-Storage-Klasse für verwaltete Cluster ändern.

Zeigen Sie den Cluster-Zustand und die Details an

Sie können Details zum Cluster anzeigen, z. B. seinen Standort, die Worker-Nodes, persistente Volumes und Storage-Klassen.

Schritte

1. Wählen Sie in der Astra Control Center-Benutzeroberfläche **Cluster** aus.
2. Wählen Sie auf der Seite **Cluster** den Cluster aus, dessen Details Sie anzeigen möchten.



Wenn ein Cluster vorhanden ist `removed` Der Zustand der Cluster- und Netzwerk-Konnektivität erscheint jedoch ordnungsgemäß (externe Versuche, mit Kubernetes-APIs erfolgreich auf das Cluster zuzugreifen, sind dennoch erfolgreich), ist das Kubeconfig, das Sie Astra Control zur Verfügung gestellt haben, möglicherweise nicht mehr gültig. Dies kann an einer Zertifikatrotation oder einem Ablaufdatum im Cluster liegen. Um dieses Problem zu beheben, aktualisieren Sie die Anmeldeinformationen, die mit dem Cluster in Astra Control verbunden sind, mithilfe des ["Astra Control API"](#).

3. Zeigen Sie die Informationen auf den Registerkarten **Übersicht**, **Speicher** und **Aktivität** an, um die gewünschten Informationen zu finden.
 - **Übersicht:** Details zu den Arbeiterknoten, einschließlich ihres Status.
 - **Storage:** Die persistenten Volumes, die mit dem Computing verbunden sind, einschließlich der Speicherklasse und des Status.
 - **Aktivität:** Zeigt die Aktivitäten im Zusammenhang mit dem Cluster an.



Sie können auch Clusterinformationen anzeigen, die Sie über das Astra Control Center **Dashboard** starten. Auf der Registerkarte **Cluster** unter **Resource summary** können Sie die verwalteten Cluster auswählen, die Sie zur Seite **Cluster** führen. Nachdem Sie die Seite **Cluster** aufgerufen haben, befolgen Sie die oben beschriebenen Schritte.

Ändern der Standard-Storage-Klasse

Sie können die Standard-Storage-Klasse für ein Cluster ändern. Wenn Astra Control einen Cluster verwaltet, wird die Standard-Storage-Klasse des Clusters überwacht.



Ändern Sie die Storage-Klasse nicht mit `kubectl`-Befehlen. Verwenden Sie stattdessen diese Prozedur. Astra Control setzt die Änderungen zurück, wenn sie mit `kubectl` vorgenommen werden.

Schritte

1. Wählen Sie in der Web-UI des Astra Control Center die Option **Cluster** aus.

2. Wählen Sie auf der Seite **Cluster** den Cluster aus, den Sie ändern möchten.
3. Wählen Sie die Registerkarte **Storage** aus.
4. Wählen Sie die Kategorie **Speicherklassen** aus.
5. Wählen Sie das Menü **Aktionen** für die Speicherklasse aus, die Sie als Standard festlegen möchten.
6. Wählen Sie **als Standard**.

Anzeigen des Funktionszustands und der Details einer App

Nachdem Sie mit dem Management einer Applikation begonnen haben, stellt Astra Control Details zur App bereit, mit der Sie ihren Status (unabhängig davon, ob sie sich gesund ist), ihren Sicherungsstatus (ob sie im Falle eines Ausfalls vollständig geschützt ist), die Behälter, den persistenten Storage und vieles mehr ermitteln können.

Schritte

1. Wählen Sie in der Astra Control Center-UI **Anwendungen** und dann den Namen einer App aus.
2. Überprüfen Sie die Informationen.
 - **App-Status:** Gibt einen Status an, der den Status der App in Kubernetes wiedergibt. Sind Pods und persistente Volumes beispielsweise online? Wenn eine Applikation fehlerhaft ist, müssen Sie mit den Kubernetes-Protokollen zum Beheben des Problems im Cluster wechseln. Astra stellt keine Informationen zur Verfügung, die Ihnen bei der Behebung einer defekten App helfen.
 - **App Protection Status:** Gibt einen Status, wie gut die App geschützt ist:
 - **Vollständig geschützt:** Die App verfügt über einen aktiven Backup-Zeitplan und ein erfolgreiches Backup, das weniger als eine Woche alt ist
 - **Teilweise geschützt:** Die App verfügt über einen aktiven Backup-Zeitplan, einen aktiven Snapshot-Zeitplan oder einen erfolgreichen Backup oder Snapshot
 - **Ungeschützt:** Apps, die weder vollständig geschützt noch teilweise geschützt sind.

__ Sie können erst dann vollständig geschützt sein, wenn Sie ein kürzlich gesichertes Backup haben. Das ist wichtig, da Backups abseits der persistenten Volumes in einem Objektspeicher gespeichert werden. Wenn ein Ausfall das Cluster herauswischt und es sich um den persistenten Storage handelt, muss das Backup wiederhergestellt werden. Ein Snapshot würde es Ihnen nicht ermöglichen, eine Wiederherstellung durchzuführen.
 - **Übersicht:** Informationen über den Zustand der Pods, die mit der App verbunden sind.
 - **Datenschutz:** Ermöglicht die Konfiguration einer Datenschutzrichtlinie und die Anzeige der vorhandenen Snapshots und Backups.
 - **Storage:** Zeigt dir die persistenten Volumes auf App-Ebene. Der Zustand eines persistenten Volumes befindet sich aus der Perspektive des Kubernetes Clusters.
 - **Ressourcen:** Ermöglicht es Ihnen, zu überprüfen, welche Ressourcen gesichert und verwaltet werden.
 - **Aktivität:** Zeigt die Aktivitäten im Zusammenhang mit der App an.



Sie können auch App-Informationen ab dem Astra Control Center **Dashboard** anzeigen. Auf der Registerkarte **Anwendungen** unter **Ressourcenzusammenfassung** können Sie die verwalteten Apps auswählen, die Sie zur Seite **Anwendungen** führen. Nachdem Sie die Seite **Applikationen** aufgerufen haben, befolgen Sie die oben beschriebenen Schritte.

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.