NetApp Console lokale Bereitstellung

NetApp Console local deployment

NetApp
August 10, 2026

Inhalt

NetApp Console lokale Bereitstellung . . . 1
- Versionshinweise . . . 1
  - Neues bei der lokalen Bereitstellung der NetApp Console . . . 1
  - Bekannte Einschränkungen bei der lokalen Bereitstellung der NetApp Console . . . 1
  - Vergleich zwischen NetApp Console lokale Bereitstellung und NetApp Console . . . 1
- Los geht’s . . . 4
  - Informationen zur lokalen Bereitstellung der NetApp Console . . . 4
  - Informationen zur Identitäts- und Zugriffsverwaltung bei der lokalen Bereitstellung der NetApp Console . . . 7
  - Informationen zum Flottenmanagement in der lokalen NetApp Console-Bereitstellung . . . 9
  - Informationen zu Speicherklassen und Richtlinien in der lokalen Bereitstellung der NetApp Console . . . 12
  - Informationen zur LLM-Integration in der lokalen NetApp Console-Bereitstellung . . . 15
  - Informationen zu NetApp Backup and Recovery in der lokalen Bereitstellung der NetApp Console . . . 16
- Installieren und einrichten . . . 17
  - Schnellstart für die Einrichtung der lokalen NetApp Console-Bereitstellung . . . 17
  - NetApp Console installieren . . . 18
  - Planung Ihrer NetApp Console-Organisation . . . 21
  - Einrichten der NetApp Console-Organisation . . . 27
  - Konsolenintegrationen und Dienste konfigurieren . . . 46
- NetApp Console verwenden . . . 54
  - Anmeldung bei der lokalen NetApp Console-Bereitstellung . . . 54
  - Zwischen Flotten in der lokalen Bereitstellung der NetApp Console wechseln . . . 55
  - Verwaltung der Benutzereinstellungen Ihrer lokalen NetApp Console-Bereitstellung . . . 56
  - Den NetApp Console-Assistenten in der NetApp Console lokalen Bereitstellung verwenden . . . 59
- Speicher in der NetApp Console verwalten . . . 60
  - Informationen zum Flottenmanagement in der lokalen NetApp Console-Bereitstellung . . . 60
  - Speicherverhalten standardisieren . . . 63
  - Speicher in der lokalen NetApp Console-Bereitstellung bereitstellen . . . 72
- Speicherzustand überwachen . . . 74
  - Speicherüberwachung in der lokalen NetApp Console-Bereitstellung . . . 74
  - Überwachung mit Dashboards . . . 75
  - Flotten mithilfe des Inventars in der lokalen NetApp Console-Bereitstellung überwachen . . . 87
  - Warnmeldungen beheben . . . 89
  - Leistungsprobleme untersuchen . . . 102
- Lokale NetApp Console-Bereitstellung verwalten und überwachen . . . 113
  - Informationen zur Administration und Überwachung in der lokalen NetApp Console-Bereitstellung . . . 113
  - Audit NetApp Console lokale Bereitstellungsaktivität . . . 114
  - NetApp Console warten . . . 115
  - Benutzer und Zugriff verwalten . . . 119
- Referenz . . . 125
  - NetApp Console API für lokale Bereitstellung . . . 125
  - Unterstützte LLM-Anbieter und Modelle in der lokalen NetApp Console-Bereitstellung . . . 126
  - ONTAP Warnungsreferenz in der NetApp Console lokalen Bereitstellung . . . 127

Cluster-Sicherheitskonformitätskategorien in der NetApp Console lokalen Bereitstellung 136
Sicherheitskonformitätskategorien für Storage-VMs in der lokalen NetApp Console-Bereitstellung 137
Wissen und Unterstützung 138
Für Support in der lokalen Bereitstellung der NetApp Console registrieren 138
Hilfe zur lokalen Bereitstellung der NetApp Console 142

NetApp Console lokale Bereitstellung

Versionshinweise

Neues bei der lokalen Bereitstellung der NetApp Console

Informationen zu den neuen Funktionen und Verbesserungen in der neuesten Version der lokalen NetApp Console-Bereitstellung.

Einführung der lokalen NetApp Console-Bereitstellung

"Lokale Bereitstellung der NetApp Console kennenlernen".

Bekannte Einschränkungen bei der lokalen Bereitstellung der NetApp Console

Bekannte Einschränkungen kennzeichnen Plattformen, Geräte oder Funktionen, die von dieser Produktversion nicht unterstützt werden oder nicht korrekt mit ihr zusammenarbeiten. Überprüfen Sie diese Einschränkungen sorgfältig.

Diese Einschränkungen gelten speziell für die Einrichtung der NetApp Console und die Administration: den Agenten, die Software-as-a-Service (SaaS) Plattform und mehr.

Einschränkungen der Console-VM

Möglicher Konflikt mit IP-Adressen in den Bereichen 10.42.0.0/16 und 10.43.0.0/16

NetApp Console lokale Bereitstellung verwendet einen festen Adressraum für die Kommunikation zwischen den Diensten. Die IP-Bereiche 10.42.0.0/16 und 10.43.0.0/16 werden für das interne Netzwerk verwendet. Vor der Bereitstellung der Console lokalen Bereitstellung ist sicherzustellen, dass diese IP-Bereiche nicht anderen VM-Instanzen, DHCP-Bereichen, DNS-Einträgen oder Load Balancer VIP-Pools in den für die Console lokale Bereitstellung verfügbaren VLANs zugewiesen sind.

Im Knowledge Base Artikel „Agent IP conflict with existing network“ finden sich Anweisungen zum Ändern der IP-Adresse der Schnittstellen des Agenten.

Shared Linux Hosts werden nicht unterstützt

Der Agent wird auf einer VM, die auch von anderen Anwendungen genutzt wird, nicht unterstützt. Die VM muss ausschließlich für die Agentensoftware reserviert sein.

Drittanbieter-Agenten und Erweiterungen

Agenten von Drittanbietern oder VM-Erweiterungen werden auf der Agent-VM nicht unterstützt.

Vergleich zwischen NetApp Console lokale Bereitstellung und NetApp Console

Die NetApp Console ist geeignet, wenn Cloud- und On-Premises-Umgebungen verwaltet werden und NetApp die Plattforminfrastruktur übernehmen soll. Die lokale Bereitstellung der NetApp Console ist geeignet, wenn eine große On-Premises ONTAP Umgebung verwaltet wird und vollständige Datenhoheit sowie richtlinienbasierte Speicherverwaltung erforderlich sind.

NetApp Console

NetApp hostet und wartet die NetApp Console als SaaS-Anwendung. Die Anmeldung erfolgt und die Speicherverwaltung kann unmittelbar beginnen. Zur Verwaltung von Speichersystemen werden schlanke Console-Agenten in Ihren Cloud- oder On-Premises-Umgebungen bereitgestellt. Die Agenten stellen eine ausgehende Verbindung zur NetApp Console-Plattform her, und NetApp übernimmt Authentifizierung, Upgrades und Verfügbarkeit der Plattform automatisch.

NetApp Console unterstützt außerdem den eingeschränkten Modus (Installation in Ihrer eigenen öffentlichen Cloud mit begrenzter ausgehender Konnektivität) und den privaten Modus (Installation lokal oder in Ihrer Cloud ohne Konnektivität zur NetApp Console-Plattform, einschließlich Air-Gap-Umgebungen).

"Erfahren Sie mehr über die Bereitstellungsmodi der NetApp Console".

NetApp Console unterstützt die breiteste Palette von Speichersystemen, einschließlich Cloud-Speicher wie Amazon FSx for ONTAP, Cloud Volumes ONTAP, Amazon S3, Google Cloud Storage, E-Series, StorageGRID und lokale ONTAP-Cluster. Es besteht Zugriff auf die vollständige Suite der NetApp Datenservices, einschließlich NetApp Backup and Recovery, NetApp Disaster Recovery, NetApp Ransomware Resilience, NetApp Copy and Sync und NetApp Data Classification. NetApp Console bietet zudem Supportvertragsfunktionen wie Digital Advisor, Lifecycle Planning und Nachhaltigkeits-Dashboards.

NetApp Console eignet sich am besten für Organisationen, die Hybrid-Cloud-Umgebungen verwalten und dabei den größtmöglichen Funktionsumfang, weniger Aufwand für den reibungslosen Betrieb und flexible Lizenzierung wünschen.

"Informationen zur NetApp Console^."

NetApp Console lokale Bereitstellung

NetApp Console lokale Bereitstellung ermöglicht den Betrieb der NetApp Console-Steuerungsebene vollständig innerhalb der eigenen lokalen Infrastruktur, ohne dass Verwaltungsdatenverkehr die Umgebung verlässt. Die Console wird als virtuelle Maschine mithilfe eines virtuellen Appliance-Images bereitgestellt und wie jede andere virtuelle Maschine in der vCenter Umgebung verwaltet. Es sind keine Console-Agenten erforderlich. Die virtuelle Maschine kommuniziert direkt mit den ONTAP Clustern.

Während der private Modus der NetApp Console auch Air-Gap- und On-Premises-Bereitstellungen unterstützt, ist die lokale Bereitstellung der Console speziell für das Management von ONTAP-Flotten im Unternehmensmaßstab konzipiert. Es werden Funktionen hinzugefügt, die in keinem NetApp Console-Bereitstellungsmodus verfügbar sind:

Speicherklassenrichtlinien
: Speicherstandards einmalig als wiederverwendbare Vorlagen definieren, die Leistungs-, Kapazitäts- und Tiering-Anforderungen bündeln. Alle Bereitstellungen verwenden genehmigte Klassen, und die lokale Bereitstellung über die Console überwacht kontinuierlich die Workloads auf Konformität und erkennt Abweichungen.

Flottenmanagement
: Cluster werden in Ordner und Flotten organisiert, die die Unternehmensstruktur widerspiegeln, anschließend kann die Administration auf Organisations-, Ordner- oder Flottenebene delegiert werden.

Workload Analyzer
: Latenz, Durchsatz, Ein-/Ausgabeoperationen pro Sekunde und Konfigurationsänderungen im Zeitverlauf korrelieren, um Leistungsprobleme zu identifizieren, bevor sie sich auf die Workloads auswirken.

Integration großer Sprachmodelle

Eine Verbindung zum eigenen großen Sprachmodell ermöglicht die Bereitstellung von Speicher mithilfe natürlicher Sprache, die Untersuchung von Warnmeldungen sowie das Erhalten kontextbezogener Antworten zur Speicherumgebung.

Geführte und automatisierte Behebung

Wenn eine Arbeitslast von ihrer Speicherklasse abweicht oder eine Warnung ausgelöst wird, bietet die lokale Bereitstellung über Console Fix-It-Empfehlungen. Geführte Schritte oder eine automatisierte Ein-Klick-Behebung ermöglichen die Wiederherstellung der Compliance ohne manuelle Schritte.

Benachrichtigung per E-Mail und Webhook

E-Mail- und Webhook-Benachrichtigungskanäle können so konfiguriert werden, dass Warnmeldungen die richtigen Teams erreichen, wenn sich die Speicherbedingungen ändern. Webhooks lassen sich in die bestehenden Überwachungs- und Incident-Management-Tools integrieren.

Die lokale Bereitstellung über die Konsole unterstützt On-Premises ONTAP Cluster sowie NetApp Backup and Recovery. Sie integriert sich in Active Directory für föderierte Authentifizierung und unterstützt Multi-Faktor-Authentifizierung für lokale Benutzer.

Die lokale Bereitstellung über die Konsole eignet sich am besten für Organisationen mit großen On-Premises ONTAP Umgebungen, die eine richtlinienbasierte Bereitstellung, automatisierte Compliance-Prüfungen und vollständige Datenhoheit benötigen.

"Informationen zur lokalen Bereitstellung der NetApp Console^."

Funktionsvergleich

Speicherverwaltung

Funktion	NetApp Console	NetApp Console lokale Bereitstellung
On-premises ONTAP Cluster	Ja (erfordert Console agent)	Ja (direkte Kommunikation von der Console-virtuellen Maschine)
Cloud-Speichersysteme (Amazon FSx for ONTAP, Cloud Volumes ONTAP, Amazon S3 und andere)	Ja	Nein
E-Series und StorageGRID	Ja	Nein
NetApp Backup and Recovery	Ja	Ja
NetApp Disaster Recovery	Ja	Nein
NetApp Ransomware Resilience	Ja	Nein
NetApp Copy and Sync	Ja	Nein
NetApp Data Classification	Ja	Nein
Digital Advisor, Lebenszyklusplanung, Nachhaltigkeit	Ja	Nein
Richtlinien für Speicherklassen und Compliance-Überwachung	Nein	Ja

Funktion	NetApp Console	NetApp Console lokale Bereitstellung
Geführte und automatisierte Behebung	Nein	Ja
Flottenmanagement (Ordner und Flotten)	Nein	Ja
Workload Analyzer	Nein	Ja
Integration großer Sprachmodelle für KI-gestützte Vorgänge	Nein	Ja

Konsoleneinrichtung und Sicherheit

Funktion	NetApp Console	NetApp Console lokale Bereitstellung
Bereitstellungsmodell	Software as a Service, gehostet von NetApp (verschiedene Bereitstellungsmodi verfügbar)	Selbstgehostete virtuelle Maschine in Ihrer eigenen Infrastruktur
Konsolenagent erforderlich	Ja	Nein
Software Upgrades	Automatisch, verwaltet von NetApp	Handbuch
Zugriff auf die Benutzeroberfläche	NetApp Console Anwendung (Internet- oder virtueller Maschinenzugriff)	Virtuelle Konsolenmaschine (lokal, keine Internetverbindung erforderlich)
Datenhoheit	Der Management-Datenverkehr geht an die NetApp Console Plattform	Kein Daten- oder Verwaltungsverkehr verlässt Ihre Umgebung
Active Directory Integration	Nein	Ja
Identitätsföderation	Ja	Nein
Multifaktor-Authentifizierung (lokale Benutzer)	Ja	Ja
Revisionsprotokollierung	Ja	Ja
Lizenzierung	Marketplace-Abonnements und Bring-Your-Own-License	Bring-your-own-License

Los geht’s

Informationen zur lokalen Bereitstellung der NetApp Console

NetApp Console lokale Bereitstellung ermöglicht das Hosten und Ausführen der NetApp Console autonomen Steuerungsebene in Ihrer eigenen Infrastruktur.

Sie erhalten einheitliches Speichermanagement, Richtliniendurchsetzung, Automatisierung im Flottenmaßstab und KI-gestützte Abläufe. Keine Daten, Metadaten oder Verwaltungsdatenverkehr verlassen Ihre Umgebung.

Console in der eigenen Infrastruktur bereitstellen und betreiben

NetApp Console lokale Bereitstellung läuft in Ihrer eigenen Infrastruktur, sodass Ihr Team Bereitstellung, Konnektivität und täglichen Betrieb kontrolliert. Sie stellen den Console Agent bereit, verwalten die Console-VM und die für den Überwachungs- und Verwaltungsdatenverkehr erforderlichen Netzwerkpfade. Dies gibt Unternehmensadministratoren die volle Kontrolle über die Betriebsgrenzen, während die Managementdaten innerhalb der Umgebung verbleiben.

- "Lokale Bereitstellung der NetApp Console mithilfe einer OVA in vCenter installieren".
- "Pflegen Sie Ihren vCenter oder ESXi-Host für die lokale Bereitstellung der NetApp Console".
- "Informationen zu den Ports für den lokalen Console Agent in der NetApp Console lokalen Bereitstellung".

Speichervorgänge mit APIs und Servicekonten automatisieren

NetApp Console lokale Bereitstellung unterstützt API-basierte Integrationen, sodass Ihr Unternehmen wiederholbare Speichervorgänge automatisieren kann. Dienstkonten ermöglichen Anwendungen die Authentifizierung und den Betrieb mit zugewiesenen Rollen. Die gleiche rollenbasierte Zugriffssteuerung und Audit-Kontrollen, die für interaktive Benutzer gelten, steuern diese Aktionen. Dies unterstützt die Unternehmensautomatisierung, während der Zugriff weiterhin gezielt und nachvollziehbar bleibt.

- "Mitglieder zur lokalen NetApp Console-Bereitstellungsorganisation hinzufügen".
- "Informationen zur API für NetApp Console IAM"

Zugriff mit rollenbasierter Zugriffssteuerung (RBAC) und Active Directory Integration steuern

NetApp Console lokale Bereitstellung bietet Zero-Trust rollenbasierte Zugriffssteuerung (RBAC), die einschränkt, was Benutzer innerhalb der von ihnen verwalteten Flotten und Ressourcen sehen und tun können. Eine Integration mit Active Directory ermöglicht es, dass sich Benutzer mit ihren bestehenden Unternehmensanmeldeinformationen anmelden, und lokale Benutzer können für eine weitere Verifizierungsebene die Multi-Faktor-Authentifizierung (MFA) hinzufügen. Die Zugriffsverwaltung bleibt mit den übergeordneten Identitäts- und Zugriffsmanagementpraktiken Ihrer Organisation abgestimmt.

- "Informationen zur Identitäts- und Zugriffsverwaltung in der lokalen NetApp Console-Bereitstellung".
- "Informationen zum sicheren Zugriff auf die lokale NetApp Console-Bereitstellung".

Flotten organisieren und Speicherverwaltung delegieren

NetApp Console lokale Bereitstellung skaliert die Administration, indem Ressourcen in Ordnern und Flotten organisiert werden. Flotten können Umgebungen, Geschäftseinheiten oder Regionen zugeordnet werden, anschließend lässt sich die Administration auf Organisations-, Ordner- oder Flottenebene delegieren, sodass die Zuständigkeiten klar bleiben. Diese Struktur hilft großen Speicherteams, Aufgaben zu verteilen, ohne die Konsistenz von Richtlinien oder die Governance zu verlieren.

- "Informationen zu Ordnern und Flotten in der lokalen Bereitstellung der NetApp Console".
- "Informationen zu Speicherflotten in der lokalen Bereitstellung der NetApp Console".

Administrative Aktivitäten für Compliance verfolgen und exportieren

Jede administrative Aktion erzeugt einen Prüfprotokolleintrag. Sicherheits- und Compliance-Teams können diese Einträge nutzen, um Vorfälle zu untersuchen, die Wirksamkeit von Kontrollmaßnahmen nachzuweisen und Prüfanforderungen zu erfüllen. Prüfprotokolle können per Webhook an Ihren Syslog-Server für zentrale Überwachung, längere Aufbewahrung und Analyse exportiert werden. Da die lokale Bereitstellung der NetApp Console in Ihrer eigenen Umgebung erfolgt, verlassen die Protokolldaten Ihre Infrastruktur niemals.

- "Audit NetApp Console lokale Bereitstellungsaktivität".

Speicher konsistent mit Speicherklassenrichtlinien bereitstellen

NetApp Console lokale Bereitstellung sorgt für einheitliches Speicherverhalten durch Speicherklassen, Vorlagen, die Leistungs-, Kapazitäts- und Tiering-Richtlinien in wiederverwendbaren Definitionen bündeln. Administratoren definieren Speicherstandards einmal. Administratoren und automatisierte Workflows verwenden diese genehmigten Klassen für alle Bereitstellungsaktivitäten in Ihrer Umgebung. Dadurch werden Konfigurationsabweichungen verhindert, der Zeitaufwand für Bereitstellungsentscheidungen durch weniger erfahrene Administratoren reduziert und sichergestellt, dass jede Arbeitslast sofort den Standards Ihres Unternehmens entspricht. Nach der Bereitstellung überwacht Console lokale Bereitstellung weiterhin jede Arbeitslast auf Konformität.

- "Informationen zur Verwaltung von Speicher mit der lokalen NetApp Console-Bereitstellung".

Die Einhaltung der Speicherklassen wird überwacht und Abweichungen automatisch behoben.

NetApp Console Local Deployment überwacht jede Arbeitslast anhand der für die Bereitstellung verwendeten Speicherklasse. Wenn eine Arbeitslast abweicht, sei es durch eine direkte Änderung der Clusterkonfiguration oder durch nachlassende Leistung, kennzeichnet NetApp Console Local Deployment den Verstoß umgehend. Administratoren können geführte Korrekturschritte nutzen oder eine automatisierte Korrektur konfigurieren, um häufige Abweichungen ohne manuelle Eingriffe zu beheben. Diese kontinuierliche Durchsetzung reduziert das Auditrisiko und hält Ihre Umgebung zwischen den geplanten Überprüfungen konform.

Speicherzustand überwachen und Benachrichtigungen für gesamte Flotten erhalten

NetApp Console lokale Bereitstellung bietet eine zentrale Stelle, um den Zustand und die Leistung aller von Ihnen verwalteten Cluster zu überwachen. Flottenweite Dashboards zeigen Cluster und Volumes an, die Aufmerksamkeit erfordern. Benutzerdefinierte Dashboards ermöglichen Administratoren die Erstellung von Überwachungsansichten, die ihren Verantwortlichkeiten entsprechen. Der Workload Analyzer korreliert Latenz, Durchsatz, Ressourcenauslastung und Konfigurationsänderungen im Zeitverlauf, um die Ursachen zu identifizieren, bevor Probleme die Workloads beeinträchtigen.

E-Mail- und Webhook-Zustellungskanäle werden so konfiguriert, dass Benachrichtigungen bei Änderungen der Bedingungen die richtigen Teams erreichen. Organisation-Administratoren richten Ziele ein, und Speicheradministratoren wenden diese in Benachrichtigungsregeln an, sodass die Reaktionswege Ihrem Betriebsmodell entsprechen. Dadurch können Enterprise-Teams schneller auf Kapazitäts-, Leistungs- und Schutzereignisse reagieren.

- "Informationen zur Überwachung des Speicherzustands in der lokalen NetApp Console-Bereitstellung".
- "Benachrichtigungszustellungskanäle in der lokalen NetApp Console-Bereitstellung einrichten".
- "Benachrichtigungsregeln für Warnungen in der lokalen NetApp Console-Bereitstellung konfigurieren".

Speicher bereitstellen und Warnmeldungen mit natürlicher Sprache untersuchen

NetApp Console lokale Bereitstellung kann mit Ihrem eigenen großen Sprachmodell (LLM) verbunden werden, um KI-gestütztes Speichermanagement bereitzustellen. Eine Arbeitslast kann in Klartext beschrieben werden, um einen Bereitstellungsplan zu erhalten, die Console kann gebeten werden, eine aktive Warnung zu untersuchen, oder es können kontextbezogene Antworten zu Ihrer Speicherumgebung abgerufen werden. Jede KI-Aktion bleibt innerhalb der Grenzen Ihrer Speicherklassen und der rollenbasierten Zugriffssteuerungen, die für Ihr Konto gelten, und sensible Vorgänge müssen vor ihrer Ausführung bestätigt werden. Console lokale Bereitstellung sendet Anfragen ausschließlich an den LLM-Endpunkt, den Ihre Administratoren konfigurieren.

- "Informationen zur LLM-Integration in der lokalen NetApp Console-Bereitstellung".

Speicher mit NetApp Backup and Recovery sichern und wiederherstellen

Neben Bereitstellung und Überwachung gibt die lokale NetApp Console-Bereitstellung Zugriff auf NetApp Backup and Recovery, sodass Sie Ihre Daten über dieselbe Oberfläche schützen können. Es besteht die Möglichkeit, Daten zu sichern und wiederherzustellen, um die Anforderungen an Schutz und Wiederherstellung zu erfüllen. Die Verwaltung des Datenschutzes zusammen mit dem Speicher sorgt für eine konsistente Governance und verringert die Anzahl der von den Teams benötigten Tools.

- "Informationen zu Datendiensten in der lokalen NetApp Console-Bereitstellung".

Informationen zur Identitäts- und Zugriffsverwaltung bei der lokalen Bereitstellung der NetApp Console

Die Identitäts- und Zugriffsverwaltung (IAM) in der lokalen NetApp Console-Bereitstellung steuert, wer sich anmelden kann, wie Identitäten verifiziert werden, auf welche Ressourcen Benutzer zugreifen können und welche Aktionen sie ausführen können. In der lokalen NetApp Console-Bereitstellung umfasst IAM rollenbasierte Zugriffssteuerung (RBAC), Multi-Faktor-Authentifizierung (MFA) und verzeichnisgestützte Authentifizierung sowie das Hierarchie- und Auditmodell, das die delegierte Administration unterstützt.

Auf dieser Seite wird das NetApp Console IAM-Modell für die lokale Bereitstellung auf hoher Ebene erläutert. Für detaillierte Beispiele zur Hierarchieplanung siehe "Informationen zu Ordnern und Flotten in der lokalen Bereitstellung der NetApp Console".

> Die Rollen *Super admin*, *Organization admin* oder *Folder or fleet admin* sind erforderlich, um IAM in der NetApp Console zu verwalten.

Was IAM in der lokalen Bereitstellung der NetApp Console bedeutet

NetApp Console lokale Bereitstellung IAM kombiniert Identitätsprüfung, Zugriffskontrolle, Delegierung und Auditierbarkeit:

- Die *Authentifizierung* bestimmt, wie sich Benutzer anmelden, entweder mit lokalen Anmeldeinformationen oder über Ihre Verzeichniskonfiguration.
- Die *Autorisierung* legt fest, was Mitglieder nach der Anmeldung tun können, basierend auf vordefinierten Rollen und dem Bereich, in dem Sie ihnen diese zuweisen.
- *Hierarchie und Zugriffsbereich* bestimmen, auf welche Ordner, Flotten und Ressourcen ein Mitglied zugreifen kann.
- Die *Mitglieder- und Berechtigungsverwaltung* legt fest, wie Benutzer und Dienstkonten hinzugefügt werden und wie MFA sowie Dienstkontogeheimnisse verwaltet werden.
- *Audit and compliance tracking* zeichnet IAM-bezogene Aktivitäten auf, sodass überprüft werden kann, wer wann die Zugriffsrechte geändert hat.

Wie die Authentifizierung funktioniert

NetApp Console lokale Bereitstellung unterstützt sowohl lokale Identitäten als auch die Integration externer Identitäten.

Sie können die lokale Bereitstellung von NetApp Console in Active Directory integrieren, sodass sich Benutzer mit ihren bestehenden Unternehmensanmeldeinformationen anmelden. Dadurch entfällt die Notwendigkeit separater Passwörter in der lokalen Console Bereitstellung, und Administratoren können Verzeichnisbenutzer beim Zuweisen von Zugriffsrechten nachschlagen.

Für lokale Benutzer fügt die Multi-Faktor-Authentifizierung (MFA) einen zusätzlichen Verifizierungsschritt hinzu, um das Risiko eines unbefugten Zugriffs zu verringern, falls die Anmeldeinformationen kompromittiert werden.

Weitere Informationen zu Authentifizierung und sicheren Anmeldeoptionen "Informationen zum sicheren Zugriff in der lokalen Bereitstellung der NetApp Console".

Funktionsweise der Autorisierung

Nach der Anmeldung eines Benutzers verwendet die lokale NetApp Console-Bereitstellung RBAC, um festzulegen, was dieser Benutzer sehen und tun kann.

Die Integration von Active Directory oder LDAP übernimmt die Authentifizierung. NetApp Console lokale Bereitstellungsautorisierung bleibt separat: Administratoren weisen vordefinierte Rollen auf Organisations-, Ordner- oder Flottenebene zu, um zu steuern, auf was jedes Mitglied zugreifen kann.

Dieselbe Rolle gewährt je nach zugewiesenem Bereich unterschiedliche Zugriffsrechte. Mit diesem Modell erhalten zentrale Administratoren umfassende Zugriffsrechte, während regionale oder Team-Administratoren auf die von ihnen verwalteten Flotten beschränkt sind.

Rollen, die Sie auf Organisations- oder Ordnerebene zuweisen, werden an untergeordnete Bereiche vererbt. Dieses Vererbungsmodell ist ein wesentlicher Bestandteil der Art und Weise, wie NetApp Console den Zugriff über Ordner und Flotten hinweg delegiert.

NetApp entwirft NetApp Console lokale Bereitstellungsrollen nach dem Prinzip der minimalen Berechtigungen, sodass jede Rolle nur die Berechtigungen enthält, die für ihre Aufgaben erforderlich sind.

"Informationen zu rollenbasierter Zugriffssteuerung und Rollenvererbung in der lokalen Bereitstellung der NetApp Console".

Wie die IAM-Hierarchie funktioniert

NetApp Console lokale Bereitstellung verwendet eine Hierarchie zur Gruppierung von Ressourcen und zur Festlegung des Zugriffsbereichs. An oberster Stelle steht die Organisation, gefolgt von Ordnern, dann Flotten und schließlich den Ressourcen (einschließlich möglicher Unterordner), die diesen Flotten zugeordnet sind.

Diese Hierarchie ermöglicht die Delegierung. Beispielsweise kann ein Organization-Administrator den Zugriff in der gesamten Organization verwalten, während ein Folder- oder Fleet-Administrator nur die Ressourcen und Mitglieder innerhalb des Teils der Hierarchie verwalten kann, den er besitzt.

NetApp Console IAM basiert auf drei Arten von Komponenten: Organisationskomponenten, die die Hierarchie definieren, Ressourcen, die innerhalb dieser Hierarchie zugewiesen werden, und Mitglieder und Rollen, die steuern, wer worauf Zugriff hat.

Da Rollen innerhalb dieser Hierarchie vererbt werden, hat Ihre Ordner- und Flottenstruktur direkten Einfluss darauf, wie weitreichend jede Zugriffszuweisung gilt.

"Informationen dazu, wie Flotten zu Ihrer Organisation hinzugefügt werden können.".

Mitgliedersicherheit und Zugangsdaten

IAM in NetApp Console lokale Bereitstellung umfasst auch operative Kontrollen zur Sicherung des Mitgliederzugriffs, nachdem Konten existieren.

Für lokale Benutzer können Administratoren die Wiederherstellung des Zugriffs unterstützen, indem sie das Zurücksetzen von Passwörtern veranlassen, die Multi-Faktor-Authentifizierung (MFA) entfernen oder vorübergehend deaktivieren und das MFA-Verhalten der lokalen Benutzer überprüfen. Für Dienstkonten können Administratoren Anmeldeinformationen neu erstellen, wenn Geheimnisse verloren gehen oder geändert werden.

Diese Kontrollmechanismen sind Teil von IAM, da sie festlegen, wie Identitäten im Laufe der Zeit geschützt bleiben und nicht nur, wie der Zugriff anfänglich zugewiesen wird.

"Informationen zur Verwaltung der Mitgliedersicherheit".

IAM-Aktivität prüfen

IAM in NetApp Console lokale Bereitstellung umfasst die Möglichkeit, zugriffsbezogene Aktivitäten zu überprüfen und zu exportieren.

Auf der Seite „Audit“ können Aktionen im Zusammenhang mit der Verwaltung Ihrer Organisation eingesehen werden, wie das Hinzufügen von Mitgliedern, das Erstellen von Flotten und das Zuordnen von Ressourcen. Audit-Protokolle können auch nach dem Tenancy Service gefiltert werden, um sich auf IAM-bezogene Änderungen zu konzentrieren, oder Audit-Protokolle können in ein externes System exportiert werden.

Die Nachvollziehbarkeit ist ein wichtiges IAM-Prinzip, da sie es ermöglicht, zu überprüfen, wer den Zugriff geändert hat, wann die Änderung erfolgte und ob die Änderung erfolgreich war.

"Informationen zur Überprüfung der lokalen Bereitstellungsaktivität der NetApp Console".

Nächste Schritte mit IAM in der NetApp Console

- "Erste Schritte mit Identität und Zugriff in der NetApp Console"
- "Informationen zum sicheren Zugriff in der lokalen Bereitstellung der NetApp Console"
- "Informationen zu RBAC in der lokalen NetApp Console-Bereitstellung"
- "Überwachung oder Prüfung der lokalen Bereitstellungsaktivität der NetApp Console"
- "Informationen zur API für NetApp Console IAM"

Informationen zum Flottenmanagement in der lokalen NetApp Console-Bereitstellung

Die Flottenverwaltung in der lokalen NetApp Console-Bereitstellung ist die Praxis, Speichersysteme in logische Gruppen zu organisieren, um einheitliche Richtlinien anzuwenden, den Zugriff zu steuern und den Zustand zusammengehöriger Cluster zu überwachen. Anstatt jeden Cluster unabhängig zu verwalten, ermöglicht die Flottenverwaltung die Behandlung Ihrer Flotte als gemeinsamen Ressourcenpool zur Unterstützung Ihrer Datenspeicherziele.

Mit zunehmender Größe Ihrer Speicherumgebung wird die Verwaltung einzelner Cluster unpraktisch. Flottenmanagement löst dieses Problem, indem eine strukturierte Möglichkeit zur Gruppierung verwandter

Systeme, zur Delegation von Verantwortlichkeiten und zur Sicherstellung des Betriebs aller Cluster nach denselben Standards geboten wird.

Warum Flottenmanagement wichtig ist

Das Flottenmanagement befasst sich mit drei zentralen Herausforderungen:

- **Vereinfachung durch Abstraktion** – Flottenmanagement abstrahiert die Komplexität der Verwaltung einzelner Speicherinfrastrukturen. Statt einer Konfiguration von Cluster zu Cluster erfolgt die Verwaltung der gesamten Speicherlandschaft als einheitliches Ganzes, wodurch der operative Aufwand und die Entscheidungsbelastung verringert werden.
- **Konsistenz und Skalierbarkeit** – Ohne klare Organisation treffen verschiedene Teams unterschiedliche Entscheidungen für ähnliche Workloads, was zu fragmentierten Konfigurationen führt. Flottenmanagement ermöglicht die gleichzeitige Anwendung von Standards auf Dutzende von Systemen und stellt so sicher, dass neue Workloads team- und flottenübergreifend auf derselben Basis beginnen.
- **Governance und Kontrolle** – Wenn Teams wachsen, sind klare Zuständigkeiten dafür erforderlich, wer was verwalten kann. Flottenmanagement schafft diese Grenzen durch Organisationsstruktur und Zugriffskontrolle, sodass Speicherentscheidungen weiterhin geregelt und nachvollziehbar bleiben.

Wie Flotten Ihre Ressourcen organisieren

Die Ressourcenhierarchie Ihrer Organisation besteht aus Ordnern und Flotten:

Eine detaillierte Übersicht über die Hierarchie und das Zugriffsmodell befindet sich unter "Informationen zu Ordnern und Flotten in der lokalen Bereitstellung der NetApp Console".

- **Organisation** – Die oberste Ebene, die Ihr Unternehmen repräsentiert.
- **Ordner** – helfen bei der Organisation zusammengehöriger Flotten. Zum Beispiel kann für jede Region oder Geschäftseinheit ein Ordner erstellt und darin Flotten angelegt werden. Ordner können weitere Ordner oder Flotten enthalten. Wird eine Rolle auf Ordnerebene zugewiesen, übernehmen die Mitglieder diese Rolle für alle Flotten innerhalb des Ordners.
- **Flotten** – Die von Ihnen verwalteten Speichersysteme werden gruppiert. Speichersysteme werden Flotten zugeordnet und Mitglieder Flotten zugewiesen, um ihnen Zugriff zu ermöglichen.

> ⓘ Ordner dienen als Organisationswerkzeug und sind für Mitglieder, die keine IAM-Berechtigungen wie Organization admin, Folder admin oder Fleet admin Rollen besitzen, nicht sichtbar. Mitglieder haben Zugriff auf Flotten, nicht auf Ordner.

Gängige Flottenorganisationsmuster

Die Organisation Ihrer Flotten hängt von Ihrem Betriebsmodell ab:

- **Nach Umgebung** – Separate Flotten für Produktions-, Entwicklungs- und Test-Workloads erstellen. So bleibt der Produktionsspeicher strengeren Richtlinien unterworfen, während in weniger anspruchsvollen Umgebungen mehr Flexibilität möglich ist.
- **Nach Geschäftsbereich** – Cluster, die einer bestimmten Abteilung wie Finanzen, Entwicklung oder Personalwesen dienen, werden zu einer dedizierten Flotte gruppiert. Speicherverwaltungsaufgaben können dann Teammitgliedern innerhalb dieses Geschäftsbereichs zugewiesen werden, ohne dass andere Flotten für sie sichtbar sind.
- **Nach Standort oder Rechenzentrum** - Wenn Cluster über mehrere Standorte verteilt sind, ermöglicht die Organisation nach Standort die Überwachung des Zustands auf Standortebene, die Anwendung

regionsspezifischer Richtlinien und die Verfolgung des Kapazitätsverbrauchs pro Standort.

- **Nach Applikations-Tier** – Cluster, die eine bestimmte Klasse von Arbeitslasten hosten, wie Datenbanken, Dateifreigaben oder virtuelle Maschinen, werden gruppiert, sodass einheitliche, auf diesen Arbeitslasttyp abgestimmte Standards für die gesamte Flotte angewendet werden können.

Ordner können verwendet werden, um eine weitere Organisationsebene hinzuzufügen. Beispielsweise kann für jede Region ein Ordner erstellt und innerhalb jedes regionalen Ordners umgebungsbasierte Flotten angelegt werden.

Wie Flottenmanagement die Zugangskontrolle ermöglicht

Flotten und Ordner dienen als Grenzen für den Benutzerzugriff und die administrative Verantwortung:

- **Zugriff auf Ordnerebene** – Wenn eine Rolle auf Ordnerebene zugewiesen wird, erbt das Mitglied diese Rolle für alle Flotten und Ressourcen innerhalb des Ordners. So ist es möglich, administrative Aufgaben zu delegieren, ohne Zugriff auf die gesamte Organisation zu gewähren.
- **Zugriff auf Flottenebene** - Bei der Zuweisung einer Rolle auf Flottenebene hat das Mitglied nur Zugriff auf die Speichersysteme innerhalb dieser Flotte. Dadurch ist es möglich, die Speicherverwaltung an Teammitglieder oder Anwendungsbesitzer zu delegieren, ohne nicht zugehörige Teile der Infrastruktur offenzulegen.

Die lokale Bereitstellung über die NetApp Console ermöglicht die Überwachung von Zustand und Leistung auf Flottenebene, sodass der Status aller Cluster einer Flotte aus einer einzigen Ansicht ersichtlich ist, Probleme frühzeitig erkannt werden und Maßnahmen ergriffen werden können, bevor sie sich auf die Workloads auswirken.

Wie das Speichermanagement funktioniert

Speichermanagement bezeichnet die Definition von Speicherstandards, deren konsistente Anwendung und den Betrieb von Workloads, sodass deren langfristige Ausrichtung erhalten bleibt. Bei der lokalen Bereitstellung über NetApp Console werden diese Standards in Form von Speicherklassenrichtlinien und Speicherklassen ausgedrückt, die Flotten zugeordnet und durch Bereitstellungs-Workflows durchgesetzt werden, die von RBAC und Audit-Protokollierung gesteuert werden.

Die lokale Bereitstellung über die Konsole verbindet vier Konzepte zu einem einzigen Workflow:

- **Flotten** definieren den Bereich, in dem Sie Speicher verwalten. Eine Flotte gruppiert Systeme, sodass Sie den Zugriff steuern, Standards einheitlich anwenden und Ressourcen als Einheit verwalten können.
- **Speicherklassenrichtlinien** definieren Standards als wiederverwendbare Bausteine (Leistung, Kapazität, Sicherheit, Datenschutz).
- **Speicherklassen** drücken die Absicht bezüglich der Arbeitslast aus. Eine Speicherklasse ist eine benannte Vorlage, die aus einer oder mehreren Richtlinien zusammengesetzt ist.
- **Bereitstellungsworkflows** erstellen Speicher innerhalb festgelegter Grenzen. Unterschiedliche Workflows treffen Konfigurationsentscheidungen auf unterschiedliche Weise, aber alle können Speicherklassen erzwingen und bleiben durch RBAC und Audit-Protokollierung geregelt.

Bereitstellungsansätze

Die lokale Bereitstellung über die Konsole unterstützt drei Bereitstellungsansätze, die alle durch RBAC, Audit-Protokollierung und Speicherklassenstandards geregelt werden:

- **Manuelle Bereitstellung** – Das Zielsystem wird ausgewählt und die Konfigurationsdetails werden direkt

angegeben. Diese Option eignet sich, wenn eine explizite Kontrolle über die Systemauswahl und Konfiguration erforderlich ist.

- **Automatisierte Bereitstellung** – Sie geben die Workload-Eingaben an und wählen optional eine Storage-Klasse aus. Die lokale Bereitstellung über die NetApp Console empfiehlt die optimale Platzierung und wendet klassenbasierte Einstellungen an, um manuelle Entscheidungen zu reduzieren.
- **KI-gestützte (agentenbasierte) Bereitstellung** – Sie beschreiben, was Sie benötigen, in natürlicher Sprache. Die lokale Bereitstellung über die Konsole schlägt einen durch RBAC und Speicherklassen eingeschränkten Plan vor und führt die Bereitstellung erst nach Ihrer Prüfung und Genehmigung durch.

Wie es weitergeht

- Informationen zu Speicherstandards sind unter "Informationen zu Speicherklassen und Richtlinien in der lokalen Bereitstellung der NetApp Console" verfügbar.
- Informationen zum Erstellen und Verwalten von Flotten sind unter "Ordner und Flotten verwalten" verfügbar.
- "Speicher manuell bereitstellen"
- "Speicher automatisch bereitstellen"
- "Speicher mit KI-Unterstützung bereitstellen"

Informationen zu Speicherklassen und Richtlinien in der lokalen Bereitstellung der NetApp Console

Eine Speicherklasse ist eine wiederverwendbare Vorlage, die das Verhalten des Speichers definiert. Bei der Bereitstellung von Speicher mithilfe einer Speicherklasse erzwingt die NetApp Console lokale Bereitstellung automatisch die in dieser Klasse kodierten Standards, ohne dass Administratoren für jede Arbeitslast individuelle Konfigurationsentscheidungen treffen müssen.

Speicherklassen basieren auf Speicherklassenrichtlinien, die einzelne Dimensionen des Speicherverhaltens definieren. Zusammen lassen sich die Speicherstandards eines Unternehmens einmalig erfassen und konsistent auf alle Flotten anwenden.

Was Speicherklassenrichtlinien sind

Eine Speicherklassenrichtlinie definiert eine Dimension des Speicherverhaltens. Richtlinien sind wiederverwendbare Bausteine, die zur Erstellung von Speicherklassen kombiniert werden.

Gängige Richtlinientypen sind:

- **Leistungsrichtlinien** – Latenzziele, IOPS oder Anforderungen an den Durchsatz definieren.
- **Kapazitätsrichtlinien** – Bereitstellungsmodus, Schwellenwertwarnungen oder Wachstumsgrenzen festlegen.
- **Sicherheitsrichtlinien** – Anforderungen an Verschlüsselung, Compliance oder Zugriffskontrolle definieren.
- **Datenschutzrichtlinien** – Snapshot-Zeitpläne, Replikationsziele oder Aufbewahrungsfristen festlegen.

Richtlinien werden unabhängig voneinander definiert und anschließend beim Erstellen einer Speicherklasse kombiniert. So lässt sich dieselbe Leistungsrichtlinie für mehrere Klassen wiederverwenden oder eine Kapazitätsrichtlinie an einer zentralen Stelle aktualisieren und diese Änderung auf alle Klassen anwenden, die sie verwenden.

Was Speicherklassen sind

Eine Speicherklasse ist eine benannte Vorlage, die aus einer oder mehreren Richtlinien zusammengestellt wird. Sie erfasst die Speicherstandards Ihrer Organisation für einen bestimmten Workload-Typ.

Beispielsweise kann eine **Production Database** Speicherklasse erstellt werden, die hohe Leistung, hohe Verfügbarkeit und strenge Datenschutzrichtlinien kombiniert, oder eine **Development File Share** Speicherklasse, die moderate Leistung, flexible Kapazität und grundlegende Datenschutzrichtlinien kombiniert.

Speicheradministratoren definieren Speicherklassen, um Unternehmensanforderungen abzubilden. Alle Bereitstellungsaktivitäten, ob manuell, über geführte Workflows oder automatisiert, greifen auf die von diesen Administratoren genehmigte Bibliothek von Klassen zurück.

Wie Speicherklassen Standards durchsetzen

Bei der Speicherbereitstellung wird eine Speicherklasse ausgewählt, anstatt einzelne Einstellungen zu konfigurieren. Die lokale Bereitstellung über die NetApp Console nutzt die Richtlinien dieser Klasse, um zu ermitteln, welche Cluster in Ihrer Flotte über ausreichende Kapazität und Leistungsreserven zur Unterstützung der Arbeitslast verfügen, die optimale Platzierungsoption zu empfehlen und klassenbasierte Einstellungen automatisch bei der Bereitstellung anzuwenden.

Nach der Bereitstellung bewertet Console local deployment kontinuierlich jede Arbeitslast anhand der Standards ihrer Speicherklasse.

Speicherklassenabweichung und Konformität

Wenn eine Arbeitslast nicht mehr der vorgesehenen Speicherklasse entspricht, wird sie von der lokalen NetApp Console-Bereitstellung zur Untersuchung und Behebung markiert.

Die Probleme lassen sich in zwei Kategorien einteilen:

- **Konfigurationsabweichung**: Die durch die Speicherklassenrichtlinie festgelegten Speichereinstellungen entsprechen nicht mehr der beabsichtigten Konfiguration. Dies kann auftreten, wenn Änderungen direkt am ONTAP Cluster oder außerhalb standardmäßiger Bereitstellungsabläufe vorgenommen werden.
- **Nichteinhaltung der Leistungsanforderungen**: Das Laufzeitverhalten der Arbeitslast entspricht nicht mehr der Performance-Absicht der Speicherklasse (zum Beispiel kontinuierlicher Druck nahe einer QoS-Grenze oder erhöhte Tail-Latenz).

Eine Analyseansicht erläutert, was sich geändert hat und warum. Geführte Korrekturmaßnahmen (zum Beispiel **Fix it**) können zur Verfügung stehen, um die Compliance wiederherzustellen. Einige Korrekturen können direkt angewendet werden, während andere möglicherweise eine Zuordnung der Workload zu einer anderen Speicherklasse erfordern, um das beabsichtigte Verhalten wiederherzustellen.

Wo untersucht werden kann

Abweichungen und Nichteinhaltungen lassen sich in der Regel von einem dieser Orte aus untersuchen (die Verfügbarkeit hängt von Ihrer Bereitstellung und Ihren Berechtigungen ab):

- **Speicherklassen:** Drift / Compliance
- **Warnungen:** Analysieren

Schritt-für-Schritt-Anweisungen sind unter Speicherklassenabweichung beheben zu finden.

End-to-End-Workflow

Die folgenden Schritte beschreiben den Prozess zur Verwendung von Speicherklassen zur Standardisierung und Steuerung des Speichers in Ihrer Umgebung:

1. **Speicherklassenrichtlinien erstellen** – Richtlinien definieren die einzelnen Dimensionen des Speicherverhaltens (Leistungsziele, Kapazitätseinstellungen, Sicherheitsanforderungen, Datensicherungszeitpläne). Richtlinien werden erstellt, bevor eine Speicherklasse aufgebaut wird.
2. **Speicherklasse erstellen** – Eine Speicherklasse wird zusammengestellt, indem jeweils eine Richtlinie aus jeder zutreffenden Kategorie kombiniert wird. Es kann eine vordefinierte Speicherklasse verwendet oder eine benutzerdefinierte Speicherklasse für die Standards Ihrer Organisation erstellt werden.
3. **Die Speicherklasse mit einer Flotte verknüpfen** - Nach dem Erstellen einer Speicherklasse erfolgt die Verknüpfung mit der Flotte, in der sie für die Bereitstellung und die Compliance-Überwachung verwendet wird.
4. **Speicherbereitstellung mithilfe der Speicherklasse** – Beim Bereitstellen eines Volumes oder einer LUN wird eine Speicherklasse ausgewählt, anstatt einzelne Einstellungen zu konfigurieren. Die lokale Bereitstellung über die Konsole verwendet die Klasse, um die optimale Clusterplatzierung zu empfehlen, anschließend erfolgt die Bereitstellung mit den in der Klasse definierten Einstellungen.
5. **Überwachung von Workloads auf Abweichungen** – Die lokale NetApp Console-Bereitstellung bewertet kontinuierlich jeden Workload anhand der in seiner Speicherklasse kodierten Standards. Treten Konfigurationsabweichungen oder eine Nichteinhaltung der Leistungsanforderungen auf, wird das Problem gekennzeichnet und möglicherweise eine Warnung ausgelöst.
6. **Abweichungen beheben, um die Konformität wiederherzustellen** - Wenn Abweichungen oder Leistungsmängel festgestellt werden, besteht die Möglichkeit, geführte Schritte zur manuellen Behebung des Problems zu nutzen, die Console lokale Bereitstellung häufige Abweichungsbedingungen automatisch beheben zu lassen oder eine Arbeitslast von ihrer Speicherklasse zu trennen, falls eine Änderung der Einstellungen erforderlich ist.

Wie Speicherklassen mit Flotten funktionieren

Speicherklassen sind Flotten zugeordnet. Wenn eine Speicherklasse einer Flotte zugeordnet wird, steht diese Klasse für alle Bereitstellungen innerhalb der Flotte zur Verfügung. Dies stellt sicher, dass jede in der Flotte bereitgestellte Workload denselben Standards folgt, wodurch Flotten die primäre Methode sind, um ein konsistentes Speicherverhalten über verwandte Cluster hinweg durchzusetzen.

Weitere Informationen zur Organisation von Flotten finden Sie unter "Informationen zum Flottenmanagement in der lokalen NetApp Console-Bereitstellung".

Wie es weitergeht

- Informationen zur Organisation der Flotte finden Sie unter "Informationen zum Flottenmanagement in der lokalen NetApp Console-Bereitstellung".
- Informationen zum Erstellen von Richtlinien und Speicherklassen sind unter "Speicherklassen und Richtlinien verwalten" zu finden.
- "Speicher manuell bereitstellen"
- "Speicher automatisch bereitstellen"
- "Speicher mit KI-Unterstützung bereitstellen"
- Zur Analyse und Behebung von Drift siehe "Speicherklassenabweichung beheben"

Informationen zur LLM-Integration in der lokalen NetApp Console-Bereitstellung

NetApp Console lokale Bereitstellung verbindet sich mit einem Large Language Model (LLM) für KI-gestütztes Speichermanagement. Nach der Einrichtung ist es möglich, Speicher mit natürlicher Sprache bereitzustellen, Warnmeldungen zu untersuchen und Speicherempfehlungen zu erhalten.

> Diese Dokumentation zur Verbindung eines LLM mit dem Konsolenassistenten zur Aktivierung von KI-Funktionen wird als Technologievorschau bereitgestellt. Mit diesem Vorschauangebot behält sich NetApp das Recht vor, Angebotsdetails, Inhalte und Zeitplan vor der allgemeinen Verfügbarkeit zu ändern.

Die KI-gestützte Verwaltung ermöglicht es Benutzern, Anfragen in einfacher Sprache zu beschreiben, während die lokale NetApp Console-Bereitstellung Ihre Speicherrichtlinien anwendet.

Die lokale Bereitstellung über die Console sendet LLM-Anfragen nur an den von Ihnen konfigurierten Endpunkt.

Was mit KI-gestütztem Speichermanagement möglich ist

Wenn die LLM-Integration aktiviert ist, stellt die lokale Bereitstellung über den NetApp Console Assistenten drei Funktionen bereit:

- **Speicherbereitstellung** Die Anforderungen an die Arbeitslast werden in einfacher Sprache beschrieben. Die lokale Bereitstellung über die NetApp Console empfiehlt und führt einen Bereitstellungsplan basierend auf den Speicherklassen aus.
- **Alarmreaktion** Die lokale NetApp Console-Bereitstellung wird aufgefordert, einen aktiven Alarm zu untersuchen. Das Problem wird analysiert und basierend auf den zugewiesenen Berechtigungen wird eine Aktion vorgeschlagen oder ausgeführt.
- **Suche und Anleitung** Es können Fragen zur Speicherumgebung oder zur ONTAP Administration gestellt werden. Die lokale NetApp Console-Bereitstellung liefert kontextbezogene Antworten aus der Dokumentation und dem aktuellen Flottenstatus.

Wählen Sie Lesezugriff oder lesen/schreiben für den NetApp Console Assistenten aus.

Nutzer wählen einen Zugriffsmodus für den Assistenten je nach gewünschtem Ergebnis:

- **Nur-Lese-Modus** zur Anleitung und Untersuchung, ohne Infrastrukturänderungen vorzunehmen.
- **Lesen/Schreiben**-Modus für die geführte Ausführung. Die lokale Bereitstellung über die NetApp Console zeigt die vorgeschlagene Aktion, fordert eine Bestätigung an und führt dann die Änderung aus.

Was die Aktionen des NetApp Console Assistenten steuert

Die lokale Bereitstellung der Console steuert die Aktionen des Console-Assistenten über dasselbe Governance-Modell, das plattformweit verwendet wird:

- Rollenbasierte Zugriffskontrollen begrenzen, was jeder Benutzer sehen und tun kann.
- Speicherrichtlinien schränken die Bereitstellung und damit verbundene Aktionen ein.
- Der Konsolenassistent verlangt eine Bestätigung, bevor er speicherverändernde Aktionen ausführt.

Einen LLM Anbieterpfad auswählen

NetApp Console lokale Bereitstellung unterstützt folgende LLM-Anbietertypen:

- **OpenAI** für den direkten Zugriff auf OpenAI Modelle.
- **OpenAI-kompatibel** für einen kompatiblen Endpunkt, wie z. B. ein Enterprise Gateway oder einen Proxy-Service.
- Anthropic für die Claude-Modelle von Anthropic.

Die Modellverfügbarkeit hängt vom konfigurierten Endpunkt ab. Ein Modell aus der Liste in der NetApp Console lokalen Bereitstellung auswählen.

Details zu den unterstützten Modellen sind unter "Informationen zu unterstützten LLM-Anbietern und Modellen in der lokalen NetApp Console-Bereitstellung" zu finden.

Verstehen, wohin LLM-Anfragen gehen

Der Datenfluss hängt vom gewählten Endpunktpfad ab:

- Wenn ein OpenAI-Endpunkt konfiguriert ist, sendet die Console lokale Bereitstellung Eingabeaufforderungen und Kontext an den OpenAI-Endpunkt.
- Wenn ein OpenAI-kompatibler Endpunkt konfiguriert wird, sendet die Console lokale Bereitstellung Eingabeaufforderungen und Kontext an den kompatiblen Endpunkt, den Ihre Organisation konfiguriert.

LLM-Zugangsdaten schützen und Administratorzugriff kontrollieren

Die Integration lässt sich mit diesen Steuerelementen schützen:

- Der API-Schlüssel ist als privilegierte Zugangsberechtigung zu behandeln und gemäß den Richtlinien Ihrer Organisation zu rotieren.
- Die Nutzung und Warnmeldungen auf Anbieterseite bieten Hinweise auf unerwartete Aktivitäten.

LLM verbinden

Nachdem diese Entscheidungen getroffen wurden, erfolgt die Fortsetzung mit "Verbinden Sie Ihren LLM und aktivieren Sie den NetApp Console Assistenten".

Falls Verbindungs- oder Laufzeitprüfungen fehlschlagen, siehe "Fehlerbehebung bei der LLM Integration".

Informationen zu NetApp Backup and Recovery in der lokalen Bereitstellung der NetApp Console

NetApp Backup and Recovery ist ein Datendienst, der effizienten, sicheren und kostengünstigen Datenschutz für alle Ihre ONTAP Workloads bietet, einschließlich Volumes, Datenbanken, virtuellen Maschinen und Kubernetes Workloads.

Eine Workload ist eine logische Gruppierung von Ressourcen innerhalb eines Systems, die als Einheit für Schutz, Verwaltung, Erkennung und Wiederherstellung verwaltet wird. Im Bereich Backup und Recovery ist eine Workload die zu schützende Einheit. Ihre Bedeutung hängt von der Datenquelle ab: In Kubernetes ist eine Workload eine Anwendung, in VM-Umgebungen eine virtuelle Maschine und in Datenbankumgebungen eine Datenbank.

Die Unterstützung für Backup und Recovery ist in allen ONTAP-Systemen bereits integriert, sodass keine zusätzliche Hardware oder Mediengateways benötigt werden. Dies macht Backup-Operationen einfach und kosteneffektiv. Die NetApp Console vereinfacht die Implementierung jeder Backup-Strategie, einschließlich des gesamten Spektrums der 3-2-1-Backup-Varianten, ohne dass mehrere Ressourcenmanager oder spezialisiertes Personal erforderlich sind.

NetApp Backup and Recovery befindet sich für die NetApp Console lokale Bereitstellung im Vorschaumodus. Der Dienst ist noch nicht allgemein verfügbar, und die Funktionen und die Funktionalität können sich ändern.

"Weitere Informationen zu NetApp Backup and Recovery.".

Installieren und einrichten

Schnellstart für die Einrichtung der lokalen NetApp Console-Bereitstellung

Nach der Installation der lokalen NetApp Console-Bereitstellung wird die Organisation so eingerichtet, dass die richtigen Teams die entsprechenden Speicherressourcen sicher verwalten können. Diese Checkliste dient zur Planung der Struktur, Organisation der Ressourcen, Hinzufügung von Mitgliedern, Konfiguration von Integrationen und Aktivierung von Datendiensten.

Erforderliche Zugriffsrollen

Super Admin oder Organisationsadministrator. "Informationen zu Zugriffsrollen".

1 **Lokale Bereitstellung der NetApp Console-Installation**

- Der Installationsablauf bietet einen Überblick über den Bereitstellungsprozess. "Informationen zum Installationsablauf für die lokale Bereitstellung der NetApp Console".
- Die lokale Bereitstellung der NetApp Console in Ihrem vCenter installieren. "Lokale Bereitstellung der NetApp Console Installation".

2 **Organisation planen**

- Wie Ordner und Flotten Ihre Ressourcen organisieren. "Informationen zu Ordnern und Flotten".
- Es wird erläutert, wie rollenbasierte Zugriffssteuerung (RBAC) Mitgliedern die benötigten Zugriffsrechte gewährt. "Informationen zur rollenbasierten Zugriffssteuerung in der lokalen NetApp Console-Bereitstellung".
- Der Workflow für Identitäts- und Zugriffsmanagement wird dargestellt. "Erste Schritte mit IAM für Flotten- und Ressourcenmanagement".

3 **Organisation einrichten**

- Fügen Sie Ihre Speichersysteme zur lokalen NetApp Console-Bereitstellung hinzu. "Speichersysteme hinzufügen".
- Die Ordner- und Flottenhierarchie wird entsprechend Ihrer Unternehmensstruktur erstellt. "Ordner und Flotten erstellen".

- Ressourcen den richtigen Ordnern und Flotten zuordnen. "Ressourcen Ordnern und Flotten zuordnen".
- Fügen Sie Mitglieder hinzu und weisen Sie ihnen ihre anfänglichen Rollen zu. "Mitglieder hinzufügen und Rollen zuweisen".

4 **Integrationen und Services konfigurieren**

- Mit Active Directory integrieren, damit Verzeichnisbenutzer auf die lokale NetApp Console-Bereitstellung zugreifen können. "Integrieren in Active Directory".
- Verbinden Sie Ihr großes Sprachmodell (LLM), um den Konsolenassistenten und die KI-gestützte Verwaltung zu aktivieren. "LLM verbinden".
- Konfiguriert wird, wie die lokale NetApp Console-Bereitstellung Benachrichtigungen zustellt. "Benachrichtigungszustellung konfigurieren".

5 **NetApp Backup and Recovery einrichten**

- "Eine Lizenz für NetApp Backup und Recovery erhalten". Sie können diesen Schritt überspringen, wenn Sie keinen Zugriff auf erweiterte Sicherungs- und Wiederherstellungsdienste benötigen.
- Die NetApp Backup and Recovery-Lizenz zur lokalen NetApp Console-Bereitstellung hinzufügen. "Die Lizenz zur lokalen Bereitstellung der NetApp Console hinzufügen".
- "Benutzern Zugriff auf NetApp Backup und Wiederherstellung gewähren".

NetApp Console installieren

Lokale Bereitstellung der NetApp Console mithilfe einer OVA in vCenter installieren

Sie verwenden eine OVA, um eine NetApp Console lokale Bereitstellung in Ihrem VCenter zu installieren. Der OVA-Download oder die URL ist über die NetApp Support-Website verfügbar.

Vorbereitung der lokalen Bereitstellung der NetApp Console zur Installation

Vor der Installation ist sicherzustellen, dass Ihr VM-Host die Anforderungen erfüllt und die NetApp Console lokale Bereitstellung auf das Internet und die Zielnetzwerke zugreifen kann. Für die Nutzung von NetApp Datenservices wie NetApp Backup und Recovery sind Cloud-Anbieter-Anmeldeinformationen für die NetApp Console lokale Bereitstellung zu erstellen, damit Aktionen in Ihrem Namen durchgeführt werden können.

Anforderungen an den lokalen Bereitstellungshost der NetApp Console prüfen

Vor der Installation der lokalen Bereitstellung von NetApp Console sollte sichergestellt sein, dass Ihr Host-Rechner die Installationsvoraussetzungen erfüllt.

- CPU: 16 Kerne oder 16 vCPUs
- RAM: 64 GB
- Speicherplatz: 596 GB (Thick Provisioning empfohlen)
- vSphere 7.0u3 oder höher, mit virtueller Hardwareversion 19 oder höher

Die lokale Bereitstellung der NetApp Console sollte in einer vCenter Umgebung und nicht direkt auf einem ESXi-Host erfolgen.

Netzwerkzugriff für die lokale Bereitstellung der NetApp Console einrichten

NetApp Console lokale Bereitstellung verwendet einen festen Adressraum für die Kommunikation zwischen den Diensten. Die IP-Bereiche 10.42.0.0/16 und 10.43.0.0/16 werden für das interne Netzwerk verwendet. Vor der Bereitstellung der Console lokalen Bereitstellung ist sicherzustellen, dass diese IP-Bereiche nicht anderen VM-Instanzen, DHCP-Bereichen, DNS-Einträgen oder Load Balancer VIP-Pools in den für die Console lokale Bereitstellung verfügbaren VLANs zugewiesen sind.

Im Knowledge Base Artikel „Agent IP conflict with existing network“ finden sich Anweisungen zum Ändern der IP-Adresse der Schnittstellen des Agenten.

Lokale Bereitstellung der NetApp Console in Ihrer vCenter-Umgebung installieren

NetApp unterstützt die lokale NetApp Console-Bereitstellung in Ihrer vCenter-Umgebung. Die OVA-Datei enthält ein vorkonfiguriertes VM-Image, das in Ihrer VMware-Umgebung bereitgestellt werden kann.

Die OVA-Datei kann heruntergeladen oder die URL kopiert werden.

Laden Sie die OVA herunter.

1. Die lokale Bereitstellungssoftware für die Konsole kann von der NetApp Support Site heruntergeladen werden.

Lokale Bereitstellung der NetApp Console in Ihrem VCenter

Melden Sie sich in Ihrer vCenter-Umgebung an, um die lokale Console-Bereitstellung durchzuführen.

Schritte

1. Das selbstsignierte Zertifikat kann in die vertrauenswürdigen Zertifikate hochgeladen werden, falls dies in Ihrer Umgebung erforderlich ist. Dieses Zertifikat kann nach der Installation ersetzt werden.
2. Die OVA kann aus der Bibliothek oder vom lokalen System bereitgestellt werden.

Vom lokalen System	Aus der Bibliothek
a. Klicken Sie mit der rechten Maustaste und wählen Sie **OVF-Vorlage bereitstellen…**. b. Wählen Sie die OVA-Datei über die URL aus oder navigieren Sie zu ihrem Speicherort, dann wählen Sie **Weiter**.	a. Gehen Sie zu Ihrer Bibliothek und wählen Sie die Console OVA aus. b. Wählen Sie **Aktionen** > **Neue VM aus dieser Vorlage**

3. Den Assistenten „OVF-Vorlage bereitstellen“ abschließen, um die Konsole bereitzustellen.
4. Einen Namen und einen Ordner für die VM auswählen, dann **Weiter** wählen.
5. Eine Rechenressource auswählen und anschließend **Weiter** wählen.
6. Die Details der Vorlage können überprüft werden, anschließend ist **Weiter** auszuwählen.
7. Die Lizenzvereinbarung wird akzeptiert, anschließend wird **Weiter** ausgewählt.
8. Wählen Sie den gewünschten Typ der Proxykonfiguration: expliziter Proxy, transparenter Proxy oder kein Proxy.

9. Wählen Sie den Datenspeicher aus, auf dem die VM bereitgestellt werden soll, und wählen Sie anschließend **Weiter**. Es sollte sichergestellt sein, dass die Host-Anforderungen erfüllt werden.
10. Wählen Sie das Netzwerk aus, mit dem die VM verbunden werden soll, und wählen Sie anschließend **Weiter**. Es ist sicherzustellen, dass das Netzwerk IPv4 ist und über ausgehenden Internetzugang zu den erforderlichen Endpunkten verfügt.
11. Im Fenster **Vorlage anpassen** sind die folgenden Felder auszufüllen:
    - **Proxyinformationen**
      - Wenn expliziter Proxy ausgewählt wurde, sind der Hostname oder die IP-Adresse und die Portnummer des Proxyservers sowie der Benutzername und das Passwort einzugeben.
      - Wenn der transparente Proxy ausgewählt wurde, ist das entsprechende Zertifikat hochzuladen.
    - **Konfiguration der virtuellen Maschine**
      - **Konfigurationsprüfung überspringen**: Dieses Kästchen ist standardmäßig deaktiviert, was bedeutet, dass die lokale NetApp Console-Bereitstellung eine Konfigurationsprüfung durchführt, um den Netzwerkzugriff zu validieren.
        - NetApp empfiehlt, dieses Kästchen nicht zu aktivieren, sodass die Installation eine Konfigurationsprüfung der NetApp Console lokalen Bereitstellung umfasst. Die Konfigurationsprüfung bestätigt, dass die NetApp Console lokale Bereitstellung Netzwerkzugriff auf die erforderlichen Endpunkte hat. Falls die Bereitstellung aufgrund von Verbindungsproblemen fehlschlägt, stehen der Validierungsbericht und die Protokolle vom Host der NetApp Console lokalen Bereitstellung zur Verfügung. In einigen Fällen kann, sofern sichergestellt ist, dass die NetApp Console lokale Bereitstellung über Netzwerkzugriff verfügt, die Prüfung übersprungen werden.
      - **Wartungskennwort**: Das Kennwort für den `maint` Benutzer festlegen, das den Zugriff auf die NetApp Console lokale Bereitstellung Wartungskonsole ermöglicht.
      - **NTP-Server**: Es können ein oder mehrere NTP-Server für die Zeitsynchronisierung angegeben werden.
      - **Hostname**: Der Hostname für diese VM wird festgelegt. Er darf die Suchdomäne nicht enthalten. Zum Beispiel sollte ein FQDN wie console10.searchdomain.company.com als console10 eingegeben werden.
      - **Primärer DNS**: Der primäre DNS-Server, der für die Namensauflösung verwendet wird, ist anzugeben.
      - **Sekundärer DNS**: Der sekundäre DNS-Server, der für die Namensauflösung verwendet wird, ist anzugeben.
      - Suchdomänen: Der Suchdomänenname ist anzugeben, der bei der Auflösung des Hostnamens verwendet wird. Wenn der FQDN beispielsweise console10.searchdomain.company.com ist, ist searchdomain.company.com einzugeben.
      - **IPv4-Adresse**: Die IP-Adresse, die dem Hostnamen zugeordnet ist.
      - **IPv4 Subnetzmaske**: Die Subnetzmaske für die IPv4-Adresse.
      - **IPv4-Gateway-Adresse**: Die Gateway-Adresse für die IPv4-Adresse.
12. **Weiter** auswählen.
13. Die Details im Fenster **Bereit zum Abschließen** können überprüft und mit **Fertigstellen** abgeschlossen werden.

    Die vSphere-Taskleiste zeigt den Fortschritt an, während die lokale NetApp Console-Bereitstellung durchgeführt wird.

14. Die VM wird eingeschaltet.

Planung Ihrer NetApp Console-Organisation

Erste Schritte mit Identität und Zugriff in der lokalen NetApp Console-Bereitstellung

Bei der lokalen Bereitstellung der NetApp Console werden die Ordner- und Flottenhierarchie eingerichtet, Mitglieder und Startberechtigungen hinzugefügt sowie Ressourcen in den richtigen Flotten platziert, sodass die entsprechenden Teams darauf zugreifen und sie verwalten können.

Erforderliche Zugriffsrollen

Superadministrator, Organisationsadministrator oder Ordner- oder Flottenadministrator. "Informationen zu Zugriffsrollen".

Für die Ersteinrichtung ist die Rolle **Organisationsadministrator** oder **Superadministrator** erforderlich. Nach der Einrichtung lassen sich Ressourcen, Mitgliederzugriffe und Flottenzugriffe entsprechend den Änderungen Ihrer Organisation verwalten.

Ressourcen hinzufügen oder entdecken

Systeme zur lokalen NetApp Console-Bereitstellung hinzufügen. Während der Ersteinrichtung werden Systeme in der Regel hinzugefügt, wenn die Standardflotte ausgewählt ist.

Informationen zum Erstellen oder Auffinden von Ressourcen:

- "On-premises ONTAP Cluster"

Erstellung der Ordner- und Flottenhierarchie

Zusätzliche Flotten und Ordner, die der Unternehmenshierarchie entsprechen, können erstellt werden.

"Informationen zur Organisation Ihrer Ressourcen mit Ordnern und Flotten".

Ressourcen den richtigen Flotten zuordnen

Beim Hinzufügen oder Erkennen eines Systems in der lokalen NetApp Console-Bereitstellung wird die Ressource automatisch der aktuell ausgewählten Flotte zugeordnet. Damit ein System den richtigen Teams zur Verfügung steht, sollte es den entsprechenden Flotten in Ihrer Hierarchie zugeordnet werden.

- "Informationen zur Verwaltung von Ressourcen in Ordnern und Flotten".

Mitglieder hinzufügen und Startberechtigungen zuweisen

Mitglieder können hinzugefügt und ihnen Rollen auf Organisations-, Ordner- oder Flottenebene entsprechend ihrer Zuständigkeit zugewiesen werden.

"Informationen zur Verwaltung von Mitgliedern und deren Berechtigungen".

Nach der Ersteinrichtung

Nach Abschluss der Ersteinrichtung können Zugriff und Ressourcenzuweisung entsprechend den Veränderungen in Ihrer Organisation verwaltet werden:

- "Ressourcen in Ordnern und Flotten verwalten"
- "Mitgliederzugriffe über Flotten und Ordner hinweg verwalten (mitgliederzentriert)"
- "Verwaltung des Zugriffs auf eine bestimmte Flotte oder einen Ordner (flottenzentriert)"
- "Ordner und Flotten löschen, wenn sie nicht mehr benötigt werden"

Verwandte Informationen

- "Informationen zum Identitäts- und Zugriffsmanagement in der NetApp Console"
- "Informationen zur API für Identität und Zugriff"

Informationen zu Ordnern und Flotten in der lokalen Bereitstellung der NetApp Console

In der lokalen NetApp Console-Bereitstellung werden Ordner und Speicherflotten verwendet, um NetApp Ressourcen zu organisieren und den Zugriff entsprechend der Unternehmensstruktur zu steuern, etwa nach Standort, Abteilung oder Workload-Typ.

Diese Seite dient Hierarchiestrategien und Flottendesignmustern. Ein vollständiges IAM-Modell mit Mitgliedern, Rollen und Ressourcenumfang befindet sich "Informationen zur Identitäts- und Zugriffsverwaltung in der lokalen NetApp Console-Bereitstellung".

Ressourcen werden in einer Hierarchie organisiert: An der Spitze steht die Organisation, dann folgen Ordner (die andere Ordner oder Flotten enthalten können) und schließlich Flotten, die Speichersysteme enthalten. Zugriffsrollen werden auf Organisations-, Ordner- oder Flottenebene zugewiesen, sodass Benutzer die passenden Zugriffsrechte auf Ressourcen erhalten.

> Sie benötigen die Rolle „Organisationsadministrator“, „Ordneradministrator“ oder „Flottenadministrator“, um Ordner und Flotten in der lokalen NetApp Console-Bereitstellung zu verwalten.

Organisationskomponenten

Die organisatorischen Komponenten (Organisation, Ordner und Flotten) bilden eine Hierarchie, die festlegt, wie Ressourcen gruppiert und wie der Zugriff delegiert wird.

Organisation

Eine Organisation bildet die oberste Ebene der NetApp Console lokalen Bereitstellungshierarchie und repräsentiert typischerweise Ihr Unternehmen. Ihre Organisation besteht aus Ordnern, Flotten, Mitgliedern, Rollen und Ressourcen. Ressourcen sind Flotten zugeordnet, und Mitgliedern werden Rollen auf Organisations-, Ordner- oder Flottenebene zugewiesen.

Ordner

Ordner gruppieren zusammengehörige Fahrzeugflotten, um sie nach Standort, Niederlassung oder Geschäftsbereich zu organisieren. Speichersysteme können nicht direkt mit Ordnern verknüpft werden, aber die Zuweisung einer Rolle auf Ordnerebene gibt einem Mitglied Zugriff auf alle Flotten in diesem Ordner.

Organisationsadministratoren können eine Ressource zu einem Ordner hinzufügen, um die Aufgabe, die Ressource Flotten zuzuordnen, an einen Ordner- oder Flottenadministrator zu delegieren. "Ressourcen mit Ordnern und Flotten verknüpfen".

Flotten

Flotten gruppieren Speichersysteme. Ressourcen werden Flotten zugeordnet und Mitgliedern Zugriff auf Flottenebene gewährt. Ressourcen können mehreren Flotten angehören. Mitglieder mit Flottenzugriff können die Ressourcen dieser Flotte verwalten.

Beispielsweise kann ein On-Premises ONTAP System je nach Bedarf entweder mit einer einzelnen Flotte oder mit allen Flotten in Ihrer Organisation verknüpft werden.

"Informationen zum Erstellen von Ordnern und Speicherflotten".

Ressourcen

Eine Ressource ist ein Speichersystem, das der lokalen Konsolenbereitstellung bekannt ist und einer Flotte zugewiesen werden kann. Eine Ressource wird einer Flotte zugeordnet, sodass Benutzer mit Zugriff auf die Flotte die Ressource verwalten können.

Sie können beispielsweise einen ONTAP Cluster einer einzelnen Flotte oder allen Flotten Ihres Unternehmens zuordnen. Wie eine Ressource zugeordnet wird, hängt von den Bedürfnissen Ihres Unternehmens ab.

"Informationen dazu, wie Ressourcen Flotten zugeordnet werden können".

Mitglieder und Rollen

Mitglieder sind die Benutzer und Dienstkonten in Ihrer Organisation. Rollen definieren, welche Aktionen sie auf welcher Hierarchieebene (Organisation, Ordner oder Flotte) ausführen können.

Mitglieder

Die Mitglieder Ihrer Organisation sind Benutzerkonten oder Dienstkonten. Ein Dienstkonto wird typischerweise von einer Anwendung verwendet, um bestimmte Aufgaben ohne menschliches Eingreifen auszuführen.

Benutzer mit der Rolle „Organisation Admin“ können neue Mitglieder zu Ihrer Organisation hinzufügen. Alle Benutzer (einschließlich Dienstkonten und Active Directory Benutzer) müssen explizit hinzugefügt und mit mindestens einer Rolle versehen werden, um auf die lokale Console Bereitstellung zugreifen zu können.

"Informationen zum Hinzufügen von Mitgliedern zu Ihrer Organisation".

Zugriffsrollen

Die lokale Bereitstellung der Konsole bietet Zugriffsrollen, die den Mitgliedern Ihrer Organisation zugewiesen werden können.

Wenn Sie einem Mitglied eine Rolle zuweisen, kann diese Rolle für die gesamte Organisation, einen bestimmten Ordner oder eine bestimmte Flotte vergeben werden. Die ausgewählte Rolle gewährt einem Mitglied Berechtigungen für die Ressourcen im ausgewählten Teil der Hierarchie.

Die lokale Bereitstellung der NetApp Console bietet granulare Rollen, die dem Prinzip der minimalen Berechtigungen folgen, was bedeutet, dass die Zugriffsrollen so gestaltet sind, dass Mitglieder nur Zugriff auf das erhalten, was sie benötigen.

Benutzer können im Zuge der Erweiterung ihrer Aufgaben mehrere Rollen übernehmen.

Rollenvererbung

Wenn Sie eine Rolle auf Organisations- oder Ordnerebene zuweisen, erben die darunter liegenden Ordner, Flotten und Ressourcen diese Rolle, sodass Ihre Ordner- und Flottenstruktur bestimmt, wie weitreichend die jeweilige Zuweisung gilt.

"Informationen zur Rollenvererbung in der lokalen Bereitstellung der NetApp Console".

Beispiele für Organisationsgestaltung

Die richtige Organisationsstruktur hängt von der Größe Ihres Unternehmens und davon ab, wie Ihre Teams organisiert sind. Die folgenden Beispiele zeigen, wie verschiedene Organisationen die Ordner- und Flottenhierarchie nutzen können, um den Zugriff effektiv zu verwalten.

Strategie für kleine Organisationen

Für Organisationen mit weniger als 50 Benutzern und zentralisierter Speicherverwaltung bietet sich ein vereinfachter Ansatz mit den Rollen Super admin und Super viewer an.

Beispiel: ABC Corporation (5-köpfiges Team)

- **Struktur**: Eine einzige Organisation mit 3 Flotten (Production, Development, Backup)
- **Rollen**:
  - 2 leitende Mitglieder: Super Admin Rolle für vollen administrativen Zugriff
  - 3 Teammitglieder: Rolle „Super viewer“ zur Überwachung ohne Änderungsrechte
- **Vorteile**: Vereinfachte Administration, reduzierte Rollenkomplexität, geeignet für Teams, die einen breiten Zugriff benötigen

Multi-regionale Unternehmensstrategie

Für große Organisationen mit regionalen Niederlassungen und spezialisierten Teams bietet sich ein hierarchischer Ansatz mit Ordnern an, die geografische oder Geschäftsbereichsgrenzen abbilden.

Beispiel: XYZ Corporation (multinationales Unternehmen)

- **Struktur**: Organisation > Regionale Ordner (Nordamerika, Europa, Asien-Pazifik) > Flotten pro Region
- **Plattformrollen**:
  - 1 Organisation Admin: Globale Aufsicht und Richtlinienmanagement
  - 3 Ordner- oder Flottenadministratoren: Regionale Kontrolle (einer pro Region)
  - 1 Federation admin: Integration des Corporate Directory Service
- **Speicherrollen nach Region**:
  - Speicheradministrator: Speichersysteme in zugewiesenen Regionen erkennen und verwalten
  - Speicheranzeige: Speicherressourcen regionsübergreifend überwachen
  - Systemgesundheitsspezialist: Speicherzustand ohne Systemänderungen verwalten
- **Vorteile**: Erhöhte Sicherheit durch Rollentrennung, regionale Autonomie und Einhaltung lokaler Vorschriften

Strategie der Fachbereichsspezialisierung

Für Organisationen mit spezialisierten Teams, die einen bestimmten Zugriff benötigen, bieten sich gezielte Rollenzuweisungen auf der Grundlage funktionaler Verantwortlichkeiten an.

Beispiel: TechCorp (mittelgroßes Technologieunternehmen)

- **Struktur**: Organisation > Abteilungsordner (IT, Sicherheit, Entwicklung) > flottenspezifische Ressourcen
- **Spezialisierte Rollen**:
  - Sicherheitsteam: Administrator für Ransomware-Resilienz und Klassifizierungs-Viewer-Rollen
  - Backup-Team: Superadministrator für Backup und Wiederherstellung für umfassende Backup-Operationen
  - Entwicklungsteam: Speicheradministrator für die Verwaltung der Testumgebung
  - Compliance-Team: Analyst für operative Unterstützung bei der Überwachung und dem Support-Fallmanagement
- **Vorteile**: Maßgeschneiderte Zugangskontrolle, verbesserte betriebliche Effizienz und klare Verantwortlichkeit für spezialisierte Aufgaben

Nächste Schritte

- "Ordner und Speicherflotten erstellen"
- "Ressourcen mit Ordnern und Flotten verknüpfen"
- "Flottenzugriffszuweisungen verwalten"
- "Überwachung oder Protokollierung von lokalen Bereitstellungsaktionen der Konsole"

Informationen zur rollenbasierten Zugriffssteuerung in der lokalen NetApp Console-Bereitstellung

Der Benutzerzugriff auf die lokale NetApp Console-Bereitstellung wird mit rollenbasierter Zugriffssteuerung (RBAC) verwaltet, wobei vordefinierte Rollen auf Organisations-, Ordner- oder Flottenebene zugewiesen werden. Jede Rolle gewährt spezifische Berechtigungen, die festlegen, welche Aktionen Benutzer innerhalb ihres zugewiesenen Bereichs ausführen können.

NetApp gestaltet Console lokale Bereitstellungsrollen nach dem Prinzip der minimalen Berechtigungen, sodass jede Rolle nur die für ihre Aufgaben erforderlichen Berechtigungen enthält. Dieser Ansatz erhöht die Sicherheit, indem der Zugriff auf das beschränkt wird, was jedes Mitglied benötigt.

Nachdem die Ressourcen in Ordnern und Flotten organisiert wurden, erhalten Organisationsmitglieder eine oder mehrere Rollen für bestimmte Ordner oder Flotten, die ihnen erlauben, ausschließlich ihre jeweiligen Verantwortlichkeiten wahrzunehmen.

Beispielsweise kann einem Mitglied die Rolle Backup and Recovery admin für eine bestimmte Flottenebene zugewiesen werden, sodass es Backup and Recovery Vorgänge für Ressourcen innerhalb dieser Flotte durchführen kann, ohne dass ihm ein umfassenderer Zugriff auf die gesamte Organisation gewährt wird. Diesem Benutzer kann dieselbe Rolle für mehrere Flotten innerhalb Ihrer Organisation zugewiesen werden.

Sie können Mitgliedern je nach ihren Verantwortlichkeiten mehrere Rollen für denselben oder unterschiedliche Verantwortungsbereiche zuweisen. Beispielsweise könnte eine kleinere Organisation demselben Mitglied sowohl die Rollen Storage admin als auch Backup and Recovery admin auf Organisationsebene zuweisen, während in einer größeren Organisation auf Flottenebene unterschiedliche Mitglieder für jede Rolle zuständig

sind.

Arten von Console Organisationsmitgliedern

NetApp Console lokale Bereitstellung unterstützt die folgenden Mitgliedertypen:

- *Benutzer*: Einzelne Benutzer können entweder lokale Benutzer sein, die zur NetApp Console lokalen Bereitstellung hinzugefügt werden und lokale Anmeldeinformationen verwenden, oder Verzeichnisbenutzer, die sich über den integrierten Active Directory- oder LDAP-Dienst authentifizieren. Beiden Benutzertypen können in der NetApp Console lokalen Bereitstellung Rollen zugewiesen werden, um auf Ressourcen zuzugreifen.
- *Dienstkonten*: Nicht-menschliche Konten, die Anwendungen oder Dienste zur Interaktion mit der lokalen NetApp Console-Bereitstellung über APIs verwenden. Dienstkonten können direkt zur lokalen Console-Bereitstellungsorganisation hinzugefügt werden.

"Informationen zum Hinzufügen von Mitgliedern zu Ihrer Organisation."

Vordefinierte Rollen in der lokalen NetApp Console-Bereitstellung

NetApp Console lokale Bereitstellung umfasst vordefinierte Rollen, die Sie Organisationsmitgliedern zuweisen können. Jede Rolle beinhaltet Berechtigungen, die festlegen, welche Aktionen ein Mitglied innerhalb seines zugewiesenen Bereichs (Organisation, Ordner oder Flotte) ausführen kann.

NetApp Console lokale Bereitstellungsrollen verwenden das Prinzip der minimalen Berechtigungen, wodurch sichergestellt wird, dass Mitglieder nur über die für ihre Aufgaben erforderlichen Berechtigungen verfügen, und kategorisieren die Rollen nach der Art des Zugriffs, den sie gewähren:

- Plattformrollen: Lokale Bereitstellungsverwaltungsberechtigungen für die NetApp Console
- Datendienstrollen: Berechtigungen für die Verwaltung spezifischer Datendienste wie Ransomware Resilience sowie Backup und Recovery
- Anwendungsrollen: Berechtigungen für die Verwaltung von Speicher sowie für die Überwachung von lokalen Bereitstellungsereignissen und Warnmeldungen der Konsole

Sie können einem Mitglied mehrere Rollen entsprechend seinen Verantwortlichkeiten zuweisen. Beispielsweise kann einem Mitglied sowohl die Rolle des Storage admin als auch die Rolle des Backup and Recovery admin für eine bestimmte Flotte zugewiesen werden.

Um den Zugriff für ein Mitglied auszuwählen, wird die Rollenkategorie den Verantwortlichkeiten des Mitglieds zugeordnet und die Rolle anschließend auf der Ebene (Organisation, Ordner oder Flotte) vergeben, die dem gewünschten Umfang des Zugriffs für das Mitglied entspricht "Informationen darüber, wie verschiedene Organisationen Rollen und Zuständigkeiten in der lokalen Bereitstellung der NetApp Console strukturieren".

"Informationen zu den vordefinierten Rollen, die Mitgliedern in der lokalen NetApp Console-Bereitstellung zugewiesen werden können".

Wie die Rollenvererbung funktioniert

Wenn Sie eine Rolle auf Organisations- oder Ordnerebene zuweisen, wird diese Rolle an die untergeordneten Bereiche innerhalb dieses Hierarchieteils vererbt. Das bedeutet, dass Rollen auf Organisationsebene organisationsweit gelten, Rollen auf Ordnerebene für alle untergeordneten Ordner und Flotten in diesem Ordner gelten und Rollen auf Flottenebene nur für die Ressourcen in dieser Flotte gelten.

Der Bereich sollte dem Zugriff entsprechen, den das Mitglied behalten soll. Beispielsweise empfiehlt sich die Zuweisung einer Rolle auf Ordnerebene, wenn das Mitglied in einer Region für mehrere Flotten denselben

Zugriff benötigt. Die Zuweisung der Rolle auf Flottenebene ist angebracht, wenn das Mitglied nur auf eine Flotte zugreifen soll.

Vererbte Zugriffsrechte können auf einer niedrigeren Ebene nicht überschrieben werden. Wenn ein Mitglied eine Rolle von der Organisation oder von einem Ordner erbt, sollte diese Zuweisung auf der höheren Ebene geändert werden, auf der sie ursprünglich erteilt wurde.

"Informationen zu Ordnern und Flotten in der lokalen Bereitstellung der NetApp Console". "Mitgliederzugriff verwalten". "Flottenzugriffszuweisungen verwalten".

Einrichten der NetApp Console-Organisation

Ordner und Flotten zur lokalen NetApp Console-Bereitstellungsorganisation hinzufügen

Ordner und Flotten können entsprechend der Unternehmensstruktur erstellt, der Zugriff gesteuert und Ressourcen in der lokalen Bereitstellung der NetApp Console organisiert werden.

Erforderliche Zugriffsrollen

Superadministrator, Organisationsadministrator oder Ordner- oder Flottenadministrator. "Informationen zu Zugriffsrollen".

NetApp Console lokale Bereitstellung erstellt beim Erstellen einer Organisation standardmäßig eine Flotte. Weitere Flotten können hinzugefügt und mit Ordnern gruppiert werden. "Informationen zur Ressourcenhierarchie in der NetApp Console".

Verwendung von Ordnern und Flotten zur Organisation von Ressourcen

Ordner und Flotten sind die beiden Bausteine, mit denen Sie Ihre Organisation so gestalten, dass sie der tatsächlichen Arbeitsweise Ihrer Teams entspricht. Beispielsweise ein Ordner pro Region mit jeweils einer Produktions- und einer Entwicklungsflotte.

- Ordner gruppieren verwandte Flotten und unterstützen die delegierte Administration sowie die Rollenvererbung.
- Flotten sind der Bereich, in dem Ressourcen für die Verwaltung zugeordnet werden und Benutzern operativer Zugriff gewährt wird.

Sie können Ordner und Flotten zuerst erstellen und Ressourcen sowie Mitgliederzugriffe später hinzufügen. Dies ermöglicht die Planung Ihrer Ressourcenhierarchie, bevor Benutzer und Ressourcen in der lokalen NetApp Console-Bereitstellung hinzugefügt werden. Wenn Ihre Struktur bereits definiert ist, können Ressourcen hinzugefügt und Zugriffsrechte zugewiesen werden, wenn die Flotte erstellt wird. Flotten können jederzeit aktualisiert werden.

Beispielsweise Produktionscluster in einer Produktionsflotte und Testcluster in einer Testflotte zusammenfassen und jedem Team nur Zugriff auf die Flotte gewähren, die es besitzt.

Ordner

Ordner organisieren Flotten nach Unternehmensstruktur, wie Geschäftsbereich, Region oder Team. Ordner können verschachtelt werden, um die Organisation widerzuspiegeln.

Auf Ordnerebene zugewiesene Rollen werden an untergeordnete Ordner und Flotten vererbt. Ein Ordner kann auch verwendet werden, um Flottenzuweisungsaufgaben an einen Ordner- oder Flottenadministrator für

diesen Teil der Hierarchie zu delegieren.

> Mitglieder arbeiten in Flotten, nicht in Ordnern. Eine Ressource, die nur einem Ordner zugeordnet ist, ist für Mitglieder erst verwaltbar, wenn sie einer Flotte zugeordnet ist.

Ein regionales Unternehmen könnte beispielsweise Ordner verwenden, um ONTAP Speicher nach Geschäftsbereich und Workload zu organisieren. Es könnte einen Hauptordner für North America, Unterordner für Production und Development sowie Flotten für ONTAP Cluster erstellen, die SAP, VMware und Backup Volumes hosten. Speicheradministratoren, die dem Ordner North America zugewiesen sind, erhalten Zugriff auf alle untergeordneten Flotten, während Anwendungsteams nur Zugriff auf die Flotten erhalten, die sie verwalten.

Flotten

Ressourcen werden Flotten zugeordnet, sodass Mitglieder sie verwalten können. Eine Flotte kann direkt unter der Organisation oder innerhalb eines Ordners existieren.

Ein Gesundheitsunternehmen nutzt beispielsweise ONTAP Storage in getrennten Produktions- und Entwicklungsumgebungen. Die Produktionsumgebung führt klinische Anwendungen und Patientenakten-Datenbanken aus, während die Entwicklungsumgebung Tests und Validierung unterstützt. Diese Trennung schützt Live-Daten, erzwingt einen strengeren Zugriff in der Produktion, unterstützt die Nachvollziehbarkeit und das Prinzip der minimalen Berechtigungen und ermöglicht es den Entwicklerteams, zu arbeiten, ohne die patientennahen Workloads zu beeinträchtigen.

Benutzer navigieren auf der Seite **Systeme** zwischen den zugewiesenen Flotten, um die mit jeder Flotte verbundenen Ressourcen zu verwalten.

Einen Ordner oder eine Flotte hinzufügen

Eine Flotte kann hinzugefügt werden, wenn ein neuer Bereich für Ressourcen und den Zugriff von Mitgliedern benötigt wird, und ein Ordner, wenn zusammengehörige Flotten gruppiert und deren Verwaltung delegiert werden sollen. Beispielsweise kann ein `Production` Ordner hinzugefügt werden, der eine `Production-US-East` Flotte und eine `Production-EU-West` weitere Flotte enthält; anschließend kann einer regionalen Leitung die Ordner- oder Flottenadministratorrolle ausschließlich für die eigene Flotte zugewiesen werden.

Sie können bis zu sieben Hierarchieebenen erstellen.

Ressourcen können hinzugefügt und Mitgliederzugriffe beim Erstellen einer Flotte oder eines Ordners zugewiesen werden, alternativ ist dies auch zu einem späteren Zeitpunkt möglich.

Schritte

1. **Verwaltung > Identität und Zugriff** auswählen.
2. **Organisation** auswählen.
3. Auf der Seite **Organisation** die Option **Ordner oder Flotte hinzufügen** auswählen.
4. **Ordner** oder **Flotte** auswählen.
5. Unter **Name und Speicherort**: Ein Name und ein Speicherort für den Ordner oder die Flotte werden eingegeben und ausgewählt.

1. Optional: Der Abschnitt **Ressourcen** kann erweitert werden, um Ressourcen mit der Flotte oder dem Ordner zu verknüpfen.
   a. Markieren Sie das Kästchen neben der Ressource, die Sie zuordnen möchten, und wählen Sie dann **Associate with the fleet**. Falls noch keine Systeme zur NetApp Console lokalen Bereitstellung

hinzugefügt wurden, ist dieser Schritt auch später möglich.

> Mitglieder können erst dann auf Ressourcen in einem Ordner zugreifen, wenn diese Ressourcen einer Flotte zugewiesen sind.

2. Optional: Der Abschnitt **Zugriff** kann erweitert werden, um Mitgliedern Zugriffsrechte zuzuweisen. **Mitglied hinzufügen** kann ausgewählt werden, um Zugriff und eine Rolle zuzuweisen. Standardmäßig hat der Benutzer, der die Flotte erstellt, Zugriff darauf.

   "Informationen zu Zugriffsrollen".

3. Wählen Sie **Add**.

Einen Ordner oder eine Flotte umbenennen

Ordner oder Flotten können bei Bedarf umbenannt werden. Die Umbenennung hat keine Auswirkungen auf zugehörige Ressourcen oder den Mitgliederzugriff.

Schritte

1. Auf der Seite **Organisation** in der Tabelle zu einer Flotte oder einem Ordner navigieren, ••• auswählen und anschließend **Ordner bearbeiten** oder **Flotte bearbeiten** wählen.
2. Auf der Seite **Bearbeiten** einen neuen Namen eingeben und **Anwenden** auswählen.

Einen Ordner oder eine Flotte löschen

Ordner und Flotten, die nicht mehr benötigt werden, können gelöscht werden, beispielsweise nach einer Teamumstrukturierung oder dem Abschluss einer Flotte.

Bevor Sie einen Ordner oder eine Flotte löschen, sind die folgenden Prüfungen abzuschließen:

- Es sollte sichergestellt sein, dass der Ordner oder die Flotte keine Ressourcen enthält. "Informationen zum Entfernen von Ressourcenverknüpfungen".
- Mitglieder, die weiterhin Zugriff auf den Ordner oder die Flotte haben, werden angezeigt. "Mitgliederzugriffszuweisungen anzeigen".
- Entfernen oder aktualisieren Sie bei Bedarf die Zugriffsrechte der Mitglieder. "Mitgliederzugriffszuweisungen ändern".
- Wenn eine Flotte gelöscht wird, sollten Ressourcen zuerst zur Zielflotte verschoben werden. "Informationen zum Verschieben von Ressourcen zwischen Flotten".

Schritte

1. Auf der Seite **Organisation** in der Tabelle zu einer Flotte oder einem Ordner navigieren, ••• auswählen und anschließend **Löschen** wählen.
2. Bestätigen Sie, dass der Ordner oder die Flotte gelöscht werden soll.

Flotten und Ordner in der lokalen NetApp Console-Bereitstellung verwalten

Nach der Ersteinrichtung sind folgende Aktionen möglich:

- **Ressourcenzuordnungen für Ordner und Flotten verwalten**: "Informationen dazu, wie Ressourcen Flotten und Ordnern zugeordnet werden können".
- **Zugriffsrechte für einen Ordner oder eine Flotte anzeigen oder aktualisieren**: "Informationen dazu, wie Benutzern Zugriff auf Flotten gewährt wird".

- **Ein Mitglied über mehrere Ordner und Flotten hinweg verwalten**: "Informationen zur Verwaltung des Mitgliederzugriffs".
- **Fügen Sie weitere Mitglieder hinzu und weisen Sie ihnen Startberechtigungen zu**: "Informationen zur Verwaltung von Mitgliedern und Berechtigungen".

Verwandte Informationen

- "Informationen zu Identität und Zugriff in der NetApp Console"
- "Erste Schritte mit Identität und Zugriff in der NetApp Console"
- "Flottenzugriffszuweisungen verwalten"
- "Informationen zur Identity and Access API"

Speichersysteme zur lokalen NetApp Console-Bereitstellung hinzufügen

Speichersysteme können zur lokalen NetApp Console-Bereitstellung hinzugefügt werden, um Überwachung, Bestandsverwaltung und Administration der Speicherinfrastruktur zu ermöglichen. Nach dem Hinzufügen eines Speichersystems erkennt die lokale Console-Bereitstellung das System und beginnt mit der Erfassung von Informationen, die für Überwachungs- und Verwaltungsaufgaben genutzt werden können.

Bevor Sie beginnen, stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen zum Hinzufügen von Speichersystemen verfügen und dass das Speichersystem von der NetApp Console lokalen Bereitstellung aus erreichbar ist.

Schritte

1. **Speicher > Verwaltung** auswählen.
2. Wählen Sie in der Dropdown-Liste „Bereich“ die Flotte aus, zu der Sie ein Speichersystem hinzufügen möchten.
3. **System hinzufügen** auswählen.
4. Geben Sie die erforderlichen Details zum Speichersystem ein, einschließlich Verbindungsinformationen und Anmeldedaten.
5. Die eingegebenen Informationen können überprüft und **Hinzufügen** ausgewählt werden.

   Das Speichersystem wird der ausgewählten Flotte hinzugefügt. Die lokale Bereitstellung über die Konsole beginnt mit der Erkennung und Überwachung des Systems. Je nach Umgebung und Netzwerkverbindung kann es einige Minuten dauern, bis das System als vollständig verwaltet angezeigt wird.

> Ein Speichersystem kann auch über die Seite **Administration > Identität und Zugriff** hinzugefügt werden, indem **System hinzufügen** ausgewählt und die erforderlichen Systeminformationen angegeben werden.

Ressourcen in Ordnern und Flotten in der lokalen NetApp Console-Bereitstellung verwalten

Der Ressourcenzugriff in der lokalen NetApp Console-Bereitstellung wird verwaltet, indem Ressourcen dem richtigen Ordner oder der richtigen Flotte zugeordnet werden, was steuert, welche Teams auf diese zugreifen und sie verwalten können.

Erforderliche Zugriffsrollen

Superadministrator, Organisationsadministrator oder Ordner- oder Flottenadministrator. "Informationen zu Zugriffsrollen".

Ressourcen können dort platziert werden, wo die richtigen Teams sie verwalten können, sie können bei einem Eigentümerwechsel verschoben und Verknüpfungen entfernt werden, wenn sie nicht mehr benötigt werden.

Eine *Ressource* ist eine Entität, die von der lokalen Console Bereitstellung erkannt wird, wie beispielsweise eine Speicherressource oder eine Backup und Recovery Workload.

Konsolenressourcentypen

Die lokale Bereitstellung über die Konsole unterstützt sowohl Speicherressourcen als auch Backup und Recovery Workloads. Entweder Speicherressourcen oder Backup und Recovery Workloads können einer Flotte zugeordnet werden, um Zugriff und Verwaltung zu steuern.

Speicherressourcen

Speicherressourcen sind die am häufigsten vorkommende Ressourcenart in Ihrem Unternehmen. Wenn ein Speichersystem zu einer lokalen Console-Bereitstellung hinzugefügt wird, sollte es einer Flotte zugeordnet werden, damit die zuständigen Teams darauf zugreifen und es verwalten können. Nach dem Hinzufügen eines ONTAP Clusters kann dieser beispielsweise der `Production-US-East` Flotte zugeordnet werden.

Backup- und Recovery-Workloads

Auch Backup and Recovery Workloads gelten als Ressourcen. Mitgliedern können Zugriffsberechtigungen für Backup and Recovery Workloads zugewiesen werden, indem die Workloads Flotten zugeordnet werden. Beispielsweise kann einem Mitglied Zugriff auf einen Backup and Recovery Workload gewährt werden, indem dieser einer Flotte zugeordnet wird, auf die das Mitglied Zugriff hat, und die entsprechende Backup and Recovery Rolle vergeben wird.

Die Ressourcen in Ihrer Organisation anzeigen

Die Ressourcen in Ihrer Organisation können angezeigt werden, um eine bestimmte Ressource zu finden und zu sehen, welchen Flotten oder Ordnern sie zugeordnet ist. Wenn noch keine Ordner oder Flotten erstellt wurden, sind alle Ressourcen direkt der Standardflotte unter der Organisation zugeordnet.

Schritte

1. **Verwaltung > Identität und Zugriff** auswählen.
2. **Ressourcen** auswählen.
3. **Erweiterte Suche & Filterung** auswählen.
4. Mit den verfügbaren Optionen lässt sich eine Ressource finden:
   - **Suche nach Ressourcennamen**: Ein Text-String kann eingegeben und **Hinzufügen** ausgewählt werden.
   - **Plattform**: Eine oder mehrere Plattformen wie Amazon Web Services können ausgewählt werden.
   - **Ressourcen**: Es können eine oder mehrere Ressourcen ausgewählt werden, wie zum Beispiel Cloud Volumes ONTAP.
   - **Organisation, Ordner oder Flotte**: Die gesamte Organisation, ein bestimmter Ordner oder eine bestimmte Flotte kann ausgewählt werden.
5. **Suchen** auswählen.

Eine Ressource mit einem Ordner oder einer Flotte verknüpfen

Eine Ressource wird einer Flotte oder einem Ordner zugeordnet, sodass die zuständigen Teams sie verwalten können. Beispielsweise kann nach dem Hinzufügen eines ONTAP Clusters dieser der `Production-US-East` Flotte zugeordnet werden, sodass die regionalen Storage-Administratoren dieser Flotte die Verwaltung übernehmen können.

Benutzer mit der Rolle „Organisationsadministrator“ können einem Ordner Ressourcen hinzufügen, um Flottenzuordnungsaufgaben an den Ordner- oder Flottenadministrator für diesen Ordner zu delegieren. "Eine Ressource mit einem Ordner verknüpfen".

Schritte

1. Auf der Seite **Ressourcen** zu einer Ressource in der Tabelle navigieren, ••• auswählen und dann **Einem Ordner oder einer Flotte zuordnen** wählen.
2. Wählen Sie einen Ordner oder eine Flotte aus und wählen Sie dann **Akzeptieren**.
3. Um einen weiteren Ordner oder eine Flotte zuzuordnen, **Ordner oder Flotte hinzufügen** auswählen und dann den Ordner oder die Flotte auswählen.

   Beachten Sie, dass Sie nur aus den Ordnern und Flotten auswählen können, für die Sie Administratorrechte besitzen.

4. **Ressourcen zuordnen** auswählen.
   - Wenn Sie die Ressource Flotten zugeordnet haben, können Mitglieder, die über Berechtigungen für diese Flotten verfügen, nun über die Console auf die Ressource zugreifen.
   - Wenn Sie die Ressource einem Ordner zugeordnet haben, kann ein *Ordner- oder Flottenadministrator* nun auf die Ressource zugreifen und sie einer Flotte innerhalb des Ordners zuordnen. "Eine Ressource mit einem Ordner verknüpfen".

Ordner und Flotten, die einem Ressourcenobjekt zugeordnet sind, anzeigen

Es kann überprüft werden, mit welchen Flotten oder Ordnern eine Ressource verknüpft ist.

Welche Mitglieder Zugriff auf die Ressource haben, lässt sich durch Überprüfung der Mitglieder feststellen, die dem zugehörigen Ordner oder der Flotte zugewiesen sind. "Flottenzugriffszuweisungen verwalten".

Schritte

1. Auf der Seite **Ressourcen** zu einer Ressource in der Tabelle navigieren, ••• auswählen und anschließend **Details anzeigen** wählen.

Das folgende Beispiel zeigt eine Ressource, die einer Flotte zugeordnet ist.

Welche Mitglieder Zugriff auf die Ressource haben, lässt sich durch Überprüfung des zugehörigen Ordners oder der Flotte feststellen.

"Flottenzugriffszuweisungen verwalten". "Mitgliederzugriff verwalten".

Eine Ressource aus einem Ordner oder einer Flotte entfernen

Die Verknüpfung einer Ressource mit einem Ordner oder einer Flotte kann entfernt werden, damit Mitglieder sie dort nicht verwalten können.

Um ein Speichersystem aus der gesamten Organisation zu entfernen, auf die Seite **Systeme** gehen und das System entfernen.

Schritte

1. Auf der Seite **Ressourcen** zu einer Ressource in der Tabelle navigieren, ••• auswählen und anschließend **Details anzeigen** wählen.
2. Um eine Ressource aus einem Ordner oder einer Flotte zu entfernen, 🗑 neben dem Ordner oder der Flotte auswählen.
3. **Löschen** auswählen, um die Verknüpfung zu entfernen.

Eine Ressource zwischen Flotten verschieben

Eine Ressource kann von einer Flotte in eine andere verschoben werden, indem ihre Zuordnung zur aktuellen Flotte entfernt und sie anschließend der Zielflotte zugeordnet wird.

Der Zugriff auf die Ressource ändert sich, sobald sich die Zuordnung ändert. Nach Möglichkeit sollten beide Schritte in einem Wartungsfenster abgeschlossen werden.

Schritte

1. Auf der Seite **Ressourcen** zu einer Ressource in der Tabelle navigieren, ••• auswählen und anschließend **Details anzeigen** wählen.
2. Wählen Sie 🗑 neben der aktuellen Flotte **Löschen** aus.
3. **Ordner oder Flotte hinzufügen** auswählen.
4. Die Zielflotte auswählen und **Akzeptieren** wählen.
5. **Ressourcen zuordnen** auswählen.

Verwandte Informationen

- "Informationen zu Identität und Zugriff in der NetApp Console"
- "Erste Schritte mit Identität und Zugriff in der NetApp Console"
- "Zugriffszuweisungen für die Flotte nach dem Verschieben von Ressourcen verwalten"
- "Informationen zur API für Identität und Zugriff"

Mitglieder zur lokalen NetApp Console-Bereitstellungsorganisation hinzufügen

Mitglieder können zur lokalen NetApp Console-Bereitstellungsorganisation hinzugefügt und Rollen zugewiesen werden, um Benutzern, Dienstkonten und Verzeichnisbenutzern Zugriff auf Organisations-, Ordner- oder Flottenebene zu ermöglichen.

Erforderliche Zugriffsrollen

Superadministrator, Organisationsadministrator oder Ordner- bzw. Flottenadministrator (für die von ihnen verwalteten Ordner und Flotten). "Informationen zu Zugriffsrollen".

Bevor Sie beginnen

- Die Ordner- und Flottenhierarchie, die zu Ihrer Organisation passt, kann erstellt werden. "Informationen zur Organisation Ihrer Ressourcen mit Ordnern und Flotten".
- Ressourcen sollten den richtigen Flotten zugeordnet werden, bevor Mitgliedern Zugriffsrechte zugewiesen werden. "Informationen zur Verwaltung von Ressourcen in Ordnern und Flotten".
- Wenn ein Verzeichnisbenutzer hinzugefügt wird, sollte zuerst der Verzeichnisdienst integriert werden. "Informationen zur Integration mit Ihrem Verzeichnisdienst.".

Informationen darüber, wie der Zugriff in der lokalen NetApp Console-Bereitstellung gewährt wird

NetApp Console verwendet rollenbasierte Zugriffssteuerung (RBAC) zur Verwaltung von Berechtigungen. Rollen werden Mitgliedern zugewiesen, um den erforderlichen Zugriff bereitzustellen. Jede Rolle definiert zulässige Aktionen für bestimmte Ressourcen.

Folgendes ist bei der Zugriffsgewährung in der lokalen NetApp Console-Bereitstellung zu beachten:

- Sie müssen jeden Benutzer explizit zu Ihrer Organisation hinzufügen und mindestens eine Rolle zuweisen, bevor dieser Benutzer auf Ressourcen zugreifen kann.
- Eine Rolle, die auf Organisations- oder Ordnerebene zugewiesen wird, wird an untergeordnete Bereiche vererbt, daher sollte der Zuweisungsbereich sorgfältig gewählt werden, damit das Mitglied nur dort Zugriff erhält, wo dies erforderlich ist. "Informationen zur Rollenvererbung in der lokalen Bereitstellung der NetApp Console".

Mitglieder zur Organisation hinzufügen

NetApp Console unterstützt drei Arten von Mitgliedern: Benutzerkonten, Verzeichnisbenutzer und Dienstkonten.

> Bevor Benutzer hinzugefügt werden können, muss zunächst ein E-Mail-Server für die lokale Bereitstellung mit Console konfiguriert werden."Informationen zur Konfiguration eines E-Mail-Servers."

Verzeichnisbenutzer authentifizieren sich über Ihren integrierten Verzeichnisdienst, jedoch muss weiterhin jeder Verzeichnisbenutzer einzeln hinzugefügt und ihm in der lokalen NetApp Console Bereitstellung Rollen zugewiesen werden. Dienstkonten werden direkt in der NetApp Console erstellt.

Allen Mitgliedern muss mindestens eine Rolle explizit zugewiesen sein, um auf die lokale NetApp Console-Bereitstellung zugreifen zu können.

Beim Hinzufügen eines Mitglieds wird die Organisation, der Ordner oder die Flotte ausgewählt, auf die das Mitglied Zugriff benötigt, und die benötigte(n) Startrolle(n) zugewiesen.

Benutzerkonto hinzufügen

Sie benötigen die Rolle „Organization admin“, „Folder admin“ oder „fleet admin“, um einen Benutzer zu einer Organisation, einem Ordner oder einer Flotte hinzuzufügen, damit dieser auf Ressourcen zugreifen kann.

Schritte

1. **Verwaltung > Identität und Zugriff** auswählen.
2. **Mitglieder** auswählen.
3. **Mitglied hinzufügen** auswählen.
4. Für **Mitgliedstyp** bleibt **Benutzer** ausgewählt.
5. Für **Benutzer-E-Mail** die E-Mail-Adresse des Benutzers angeben, die mit dem von ihm erstellten Login verknüpft ist.
6. Im Abschnitt **Organisation, Ordner oder Flotte auswählen** wird ausgewählt, wo das Mitglied Zugriff benötigt.

   Dabei ist Folgendes zu beachten:

   - Sie können nur die Ordner und Flotten auswählen, für die Sie Berechtigungen haben.
   - Wenn Sie eine Organisation oder einen Ordner auswählen, erteilen Sie dem Mitglied Berechtigungen für alle darin enthaltenen Inhalte.
   - Die Rolle **Organization admin** kann nur auf Organisationsebene zugewiesen werden.
7. **Wählen Sie eine Kategorie** und wählen Sie dann eine **Rolle** aus, die dem Mitglied die erforderlichen Startberechtigungen für die von Ihnen ausgewählte Organisation, den Ordner oder die Flotte zuweist.

   "Informationen zu Zugriffsrollen".
8. Um Zugriff auf weitere Ordner, Flotten oder Rollen zu gewähren, **Rolle hinzufügen** auswählen, die Ordner-, Flotten- oder Rollenkategorie wählen und eine Rolle auswählen.
9. Wählen Sie **Add**.

   Die Konsole sendet dem Benutzer eine E-Mail mit Anweisungen.

Ein Dienstkonto hinzufügen

Ein Dienstkonto wird hinzugefügt, wenn Aufgaben automatisiert oder eine sichere Verbindung zu den Console-APIs hergestellt werden soll. Nach der Erstellung des Kontos sind die Client-ID und das Client-Geheimnis für die Integration zu kopieren, die dieses Konto verwendet.

Schritte

1. **Verwaltung > Identität und Zugriff** auswählen.
2. **Mitglieder** auswählen.
3. **Mitglied hinzufügen** auswählen.
4. Für **Mitgliedstyp** die Option **Dienstkonto** auswählen.
5. Geben Sie einen Namen für das Servicekonto ein.
6. Im Abschnitt **Organisation, Ordner oder Flotte auswählen** wird ausgewählt, wo das Dienstkonto Zugriff benötigt.

   Dabei ist Folgendes zu beachten:

   - Sie können nur aus den Ordnern und Flotten auswählen, für die Sie Berechtigungen haben.
   - Durch die Auswahl einer Organisation oder eines Ordners erhält das Mitglied Berechtigungen für alle darin enthaltenen Inhalte.

- Die Rolle **Organization admin** kann nur auf Organisationsebene zugewiesen werden.

7. Eine **Kategorie** auswählen und dann eine **Rolle** auswählen, die dem Dienstkonto die erforderlichen Startberechtigungen für die ausgewählte Organisation, den Ordner oder die Flotte zuweist.

   "Informationen zu Zugriffsrollen".

8. Um Zugriff auf weitere Ordner, Flotten oder Rollen zu gewähren, **Rolle hinzufügen** auswählen, die Ordner-, Flotten- oder Rollenkategorie wählen und eine Rolle auswählen.
9. Die Client-ID und das Client-Geheimnis können heruntergeladen oder kopiert werden.

   Die Konsole zeigt das Client-Geheimnis nur einmal an. Es sollte sicher kopiert werden; eine spätere Neuerstellung ist möglich, falls es verloren geht.

10. **Schließen** auswählen.

Einen Verzeichnisbenutzer zur Organisation hinzufügen

Fügen Sie einen Benutzer aus Ihrem integrierten Verzeichnisdienst hinzu und weisen Sie ihm die ersten Rollen zu. Beispielsweise kann ein neuer Speichertechniker aus Active Directory hinzugefügt und die Rolle Storage admin für die `Production-US-East` fleet zugewiesen werden, sodass er in dieser fleet arbeiten kann.

Sie müssen zuerst Ihren Verzeichnisdienst konfigurieren, bevor Sie Verzeichnisbenutzer hinzufügen können. "Informationen zur Integration mit Ihrem Verzeichnisdienst.".

Schritte

1. **Verwaltung > Identität und Zugriff** auswählen.
2. **Mitglieder** auswählen.
3. **Mitglied hinzufügen** auswählen.
4. Für **Mitgliedstyp** die Option **Verzeichnisbenutzer** auswählen.
5. Für **Benutzer-E-Mail** ist die E-Mail-Adresse des Verzeichnisbenutzers einzugeben, den Sie hinzufügen möchten. Diese E-Mail-Adresse muss mit der E-Mail-Adresse übereinstimmen, die mit dem Login des Benutzers in Ihrem Verzeichnis verknüpft ist.
6. Im Abschnitt **Organisation, Ordner oder Flotte auswählen** wird ausgewählt, wo der Verzeichnisbenutzer Zugriff benötigt.

   Dabei ist Folgendes zu beachten:

   - Sie können nur aus den Ordnern und Flotten auswählen, für die Sie Berechtigungen haben.
   - Durch die Auswahl einer Organisation oder eines Ordners erhält das Mitglied Berechtigungen für alle darin enthaltenen Inhalte.
   - Die Rolle **Organization admin** kann nur auf Organisationsebene zugewiesen werden.

7. Wählen Sie eine **Kategorie** aus und anschließend eine **Rolle**, die dem Verzeichnisbenutzer die erforderlichen Startberechtigungen für die von Ihnen ausgewählte Organisation, den Ordner oder die Flotte erteilt.

   "Informationen zu Zugriffsrollen".

8. Um dem Benutzer zusätzlichen Zugriff auf andere Ordner, Flotten oder Rollen zu geben, **Rolle hinzufügen** auswählen, den Ordner oder die Flotte, die Rollenkategorie und eine Rolle auswählen.

Zugriffsrollen

NetApp Console lokale Bereitstellungszugriffsrollen

Die Identitäts- und Zugriffsverwaltung (IAM) in der lokalen NetApp Console-Bereitstellung bietet vordefinierte Rollen, die Sie den Mitgliedern Ihrer Organisation auf verschiedenen Ebenen Ihrer Ressourcenhierarchie zuweisen können. Vor der Zuweisung dieser Rollen ist es wichtig, die Berechtigungen jeder einzelnen Rolle zu verstehen. Rollen lassen sich in folgende Kategorien einteilen: Plattform, Anwendung und Datendienst.

Plattformrollen

Plattformrollen gewähren Administrationsberechtigungen für die lokale Bereitstellung der NetApp Console, einschließlich Rollenzuweisung und Benutzerverwaltung. Die lokale Bereitstellung der Console verfügt über mehrere Plattformrollen.

Plattformrolle	Verantwortlichkeiten
"Organisationsadministrator"	Diese Rolle ermöglicht es einem Benutzer, uneingeschränkten Zugriff auf alle Flotten und Ordner innerhalb einer Organisation zu erhalten, Mitglieder zu beliebigen Flotten oder Ordnern hinzuzufügen sowie alle Aufgaben auszuführen und alle Datendienste zu nutzen, denen keine explizite Rolle zugeordnet ist. Benutzer mit dieser Rolle verwalten die Organisation, indem sie Ordner und Flotten erstellen, Rollen zuweisen, Benutzer hinzufügen und Systeme verwalten, sofern sie über die entsprechenden Anmeldeinformationen verfügen.
"Ordner- oder Flottenadministrator"	Gewährt einem Benutzer uneingeschränkten Zugriff auf zugewiesene Flotten und Ordner. Kann Mitglieder zu den von ihm verwalteten Ordnern oder Flotten hinzufügen sowie beliebige Aufgaben ausführen und jeden Datendienst oder jede Anwendung auf Ressourcen innerhalb des zugewiesenen Ordners oder der Flotte nutzen.
"Federation Admin"	Ermöglicht einem Benutzer, Verzeichnisdienstföderationen mit der Console zu erstellen und zu verwalten, sodass sich Benutzer mit ihren bestehenden Verzeichnisanmeldeinformationen authentifizieren können.
"Federation Viewer"	Ermöglicht einem Benutzer, bestehende Verzeichnisdienstverbünde mit der Console anzuzeigen. Kann keine Verbünde erstellen oder verwalten.
"Super-Admin"	Gewährt dem Benutzer alle Administratorrechte. Diese Rolle ist für kleinere Organisationen konzipiert, die die Konsolenverantwortung möglicherweise nicht auf mehrere Benutzer verteilen müssen.
"Superbetrachter"	Gewährt dem Benutzer alle Betrachterrollen. Diese Rolle ist für kleinere Organisationen konzipiert, die die Verantwortung für die NetApp Console möglicherweise nicht auf mehrere Benutzer verteilen müssen.

Anwendungsrollen

Nachfolgend ist eine Liste der Rollen in der Anwendungskategorie aufgeführt. Jede Rolle gewährt spezifische Berechtigungen innerhalb ihres festgelegten Bereichs. Benutzer ohne die erforderliche Anwendungs- oder Plattformrolle haben keinen Zugriff auf die jeweilige Anwendung.

Anwendungsrolle	Verantwortlichkeiten
"Analyst für operative Unterstützung"	Bietet Zugriff auf Warnmeldungen und Überwachungstools wie die Audit-Seite.
"Speicheradministrator"	Speicherzustands- und Governance-Funktionen verwalten, Speicherressourcen erkennen sowie bestehende Systeme ändern und löschen.
"Speicherbetrachter"	Speicherzustand und Verwaltungsfunktionen einsehen sowie zuvor erkannte Speicherressourcen anzeigen. Bestehende Speichersysteme können nicht erkannt, geändert oder gelöscht werden.
"System-Health-Spezialist"	Verwaltung von Speicher-, Systemzustands- und Governance-Funktionen, alle Berechtigungen des Storage-Administrators, jedoch ohne die Möglichkeit, bestehende Systeme zu ändern oder zu löschen.

Datendienstrollen

Nachfolgend ist eine Liste der Rollen in der Kategorie Datendienste aufgeführt. Jede Rolle gewährt spezifische Berechtigungen innerhalb ihres festgelegten Bereichs. Benutzer, die nicht über die erforderliche Datendienstrolle oder eine Plattformrolle verfügen, haben keinen Zugriff auf den Datendienst.

Datendienstrolle	Verantwortlichkeiten
"Backup und Recovery Superadministrator"	Beliebige Aktionen in NetApp Backup and Recovery ausführen.
"Backup und Recovery Administrator"	Backups auf lokale Snapshots durchführen, auf sekundären Speicher replizieren und auf Objektspeicher sichern.
"Backup und Recovery Restore-Administrator"	Stellen Sie Workloads in der Sicherung und Wiederherstellung wieder her.
"Backup and Recovery Klonadministrator"	Anwendungen und Daten in der Backup and Recovery klonen.
"Backup und Recovery-Anzeige"	Informationen zu Backup und Recovery anzeigen.
Klassifizierungsbetrachter	Ermöglicht Benutzern, NetApp Data Classification-Scanergebnisse anzuzeigen. Benutzer mit dieser Rolle können Compliance-Informationen anzeigen und Berichte für Ressourcen generieren, auf die sie Zugriff haben. Diese Benutzer können das Scannen von Volumes, Buckets oder Datenbankschemata nicht aktivieren oder deaktivieren. Data Classification hat keine Admin-Rolle.
SnapCenter Admin	Ermöglicht das Sichern von Snapshots lokaler ONTAP-Cluster mithilfe von NetApp Backup and Recovery für Anwendungen. Ein Mitglied mit dieser Rolle kann die folgenden Aktionen ausführen: * Jede Aktion aus Backup and Recovery > Applications ausführen * Alle Systeme in den Flotten und Ordnern verwalten, für die Berechtigungen bestehen * Alle NetApp Console Services nutzen SnapCenter hat keine Viewer-Rolle.

Verwandte Links

- "Erfahren Sie mehr über das NetApp Console-Identitäts- und Zugriffsmanagement"
- "Erste Schritte mit Identität und Zugriff in der NetApp Console"

- "Mitglieder hinzufügen und Rollen in einer NetApp Console-Organisation zuweisen"
- "Informationen zur API für NetApp Console IAM"

NetApp Console Zugriffsrollen für die lokale Bereitstellungsplattform

Plattformrollen werden Benutzern zugewiesen, um Berechtigungen für die Verwaltung der lokalen NetApp Console-Bereitstellung, die Rollenzuweisung, das Hinzufügen von Benutzern, das Erstellen von Flotten und die Verwaltung der Benutzerauthentifizierung zu erhalten.

Beispiel für Organisationsrollen für eine große multinationale Organisation

Die XYZ Corporation organisiert den Datenspeicherzugriff nach Regionen (Nordamerika, Europa und Asien-Pazifik) und bietet regionale Kontrolle mit zentralisierter Aufsicht.

Der **Organisationsadministrator** in der lokalen Bereitstellung der XYZ Corporation Console erstellt eine initiale Organisation und separate Ordner für jede Region. Der **Ordner- oder Flottenadministrator** jeder Region organisiert Flotten (mit zugehörigen Ressourcen) innerhalb des jeweiligen Regionsordners.

Regionale Administratoren mit der Rolle **Ordner- oder Flottenadministrator** verwalten ihre Ordner aktiv, indem sie Ressourcen und Benutzer hinzufügen. Diese regionalen Administratoren können außerdem Ordner und Flotten, die sie verwalten, hinzufügen, entfernen oder umbenennen. Der **Organisationsadministrator** erbt die Berechtigungen für alle neuen Ressourcen und behält die Übersicht über die Speichernutzung in der gesamten Organisation.

Innerhalb derselben Organisation wird einem Benutzer die Rolle **Verbundadministrator** zugewiesen, um den Verbund der Organisation mit dem zentralen Identitätsanbieter (IdP) zu verwalten. Dieser Benutzer kann Verbundorganisationen hinzufügen oder entfernen, jedoch keine Benutzer oder Ressourcen innerhalb der Organisation verwalten. Der **Organisationsadministrator** weist einem Benutzer die Rolle **Verbundbetrachter** zu, um den Verbundstatus zu überprüfen und Verbundorganisationen anzuzeigen.

Die folgenden Tabellen zeigen die Aktionen, die jede Rolle der lokalen Console Bereitstellungsplattform ausführen kann.

Organisationsverwaltungsrollen

Aufgabe	Organisationsadministrator	Ordner- oder Flottenadministrator
Systeme aus der lokalen NetApp Console-Bereitstellung erstellen, ändern oder löschen (Systeme hinzufügen oder erkennen)	Ja	Ja
Ordner und Flotten erstellen und löschen	Ja	Nein
Vorhandene Ordner und Flotten umbenennen	Ja	Ja
Rollen zuweisen und Benutzer hinzufügen	Ja	Ja
Ressourcen mit Ordnern und Flotten verknüpfen	Ja	Ja
Registrierung für Support und Einreichung von Fällen über die Konsole erfolgen über die Console.	Ja	Ja
Datendienste nutzen, die keiner expliziten Zugriffsrolle zugeordnet sind	Ja	Ja

Aufgabe	Organisationsadministrator	Ordner- oder Flottenadministrator
Die Seite „Audit“ und die Benachrichtigungen werden angezeigt	Ja	Ja

Föderationsrollen

Aufgabe	Federation Admin	Federation Viewer
Verzeichnisdienstintegrationen erstellen und aktualisieren	Ja	Nein
Verbände und deren Details	Ja	Ja

Super Admin- und Betrachterrollen

Die Rolle **Super admin** bietet vollen Zugriff auf die Verwaltung von Console-Funktionen, Storage und Data Services. Diese Rolle eignet sich für Personen, die für Administration und Governance verantwortlich sind. Im Gegensatz dazu bietet die Rolle **Super viewer** nur Lesezugriff und ist ideal für Prüfer oder Stakeholder, die Einblick benötigen, ohne Änderungen vorzunehmen.

Organisationen sollten den **Super admin**-Zugriff sparsam einsetzen, um Sicherheitsrisiken zu minimieren und dem Prinzip der minimalen Berechtigungen zu entsprechen. Die meisten Organisationen sollten fein abgestufte Rollen mit nur den notwendigen Berechtigungen vergeben, um Risiken zu reduzieren und die Nachvollziehbarkeit zu verbessern.

Beispiel für Superrollen

Die ABC Corporation verfügt über ein kleines Team von fünf Mitarbeitenden, das die NetApp Console für Datendienste und Speichermanagement nutzt. Anstatt mehrere Rollen zu vergeben, wird die Rolle **Super admin** zwei erfahrenen Teammitgliedern zugewiesen, die alle administrativen Aufgaben einschließlich Benutzermanagement und Ressourcenkonfiguration übernehmen. Die übrigen drei Teammitglieder erhalten die Rolle **Super viewer**, wodurch sie den Speicherzustand und den Status der Datendienste überwachen können, ohne Einstellungen ändern zu können.

Rolle	Geerbte Rollen
Super-Admin	• Organisationsadministrator • Ordner- oder Flottenadministrator • Backup und Recovery Superadministrator • Speicheradministrator
Superbetrachter	• Organisationsansicht • Backup Viewer • Speicherbetrachter

Zugriffsrolle für den Operational Support Analyst in der lokalen NetApp Console-Bereitstellung

In der lokalen Bereitstellung von NetApp Console kann die Rolle des Operational support analyst Benutzern zugewiesen werden, um ihnen Zugriff auf Warnmeldungen und Überwachung zu ermöglichen.

Analyst für operative Unterstützung

Aufgabe	Kann ausführen
Speichersysteme anzeigen	Ja
Die Seite „Audit“ und die Benachrichtigungen werden angezeigt	Ja
Benachrichtigungen anzeigen, herunterladen und konfigurieren	Ja

Speicherzugriffsrollen für die lokale NetApp Console-Bereitstellung

Sie können Benutzern die folgenden Rollen zuweisen, um ihnen Zugriff auf die Speicherverwaltungsfunktionen in der lokalen NetApp Console-Bereitstellung zu ermöglichen. Benutzern kann eine administrative Rolle zur Speicherverwaltung oder eine Betrachterrolle zur Überwachung zugewiesen werden.

Administratoren können Benutzern Speicherrollen für die folgenden Speicherressourcen und Funktionen zuweisen:

Speicherressourcen:

- On-premises ONTAP Cluster

Konsolendienste und Funktionen:

- Speicherzustandsfunktionen

Beispiel für Speicherrollen in der lokalen NetApp Console-Bereitstellung

Die multinationale XYZ Corporation verfügt über ein großes Team von Storage Engineers und Storage Administrators. Dieses Team kann Speicherressourcen für seine Regionen verwalten, während der Zugriff auf zentrale lokale Aufgaben der Console wie Benutzerverwaltung und Lizenzverwaltung eingeschränkt bleibt.

Innerhalb eines 12-köpfigen Teams erhalten zwei Benutzer die Rolle **Storage viewer**, mit der sie die Speicherressourcen der ihnen zugewiesenen Console local deployment fleets überwachen können. Die übrigen neun erhalten die Rolle **Storage admin**, die die Verwaltung von Software-Updates, den Zugriff auf ONTAP System Manager über die Console local deployment sowie das Erkennen von Speicherressourcen (Hinzufügen von Systemen) umfasst. Ein Teammitglied erhält die Rolle **System health specialist**, sodass die Person den Zustand der Speicherressourcen in ihrer Region verwalten kann, jedoch keine Systeme ändern oder löschen darf. Diese Person kann außerdem Software-Updates für die Speicherressourcen der ihr zugewiesenen Flotten durchführen.

Die Organisation verfügt über zwei weitere Benutzer mit der Rolle **Organization admin**, die alle Aspekte der Console lokalen Bereitstellung verwalten können, einschließlich Benutzerverwaltung und Lizenzverwaltung, sowie über mehrere Benutzer mit der Rolle **Folder or fleet admin**, die Verwaltungsaufgaben für die Console

lokale Bereitstellung für die ihnen zugewiesenen Ordner und Flotten durchführen können.

Die folgende Tabelle zeigt die Aktionen, die jede Speicherrolle ausführt.

Funktion und Aktion	Speicheradministrator	System-Health-Spezialist	Speicherbetrachter
Speicherverwaltung:			
Neue Ressourcen entdecken (Systeme hinzufügen)	Ja	Ja	Nein
Hinzugefügte Systeme anzeigen	Ja	Ja	Nein
Systeme aus der Console löschen	Ja	Nein	Nein
Systeme ändern	Ja	Nein	Nein
System Manager Zugriff			
Kann Anmeldeinformationen eingeben	Ja	Ja	Nein

NetApp Backup and Recovery Rollen in der lokalen NetApp Console Bereitstellung

In der lokalen NetApp Console-Bereitstellung können Sie Benutzern die folgenden Rollen zuweisen, um ihnen Zugriff auf NetApp Backup and Recovery innerhalb der Console zu ermöglichen. Backup and Recovery-Rollen bieten die Flexibilität, Benutzern eine Rolle zuzuweisen, die genau auf die Aufgaben zugeschnitten ist, die sie in Ihrem Unternehmen erfüllen müssen. Wie Rollen zugewiesen werden, hängt von den eigenen Geschäfts- und Speichermanagementpraktiken ab.

Der Dienst verwendet die folgenden Rollen, die speziell für NetApp Backup and Recovery vorgesehen sind.

- **Superadministrator für Backup und Recovery**: Beliebige Aktionen in NetApp Backup and Recovery ausführen.
- **Backup and Recovery Backup-Administrator**: Backups auf lokale Snapshots durchführen, auf sekundären Speicher replizieren und in Objektspeicher sichern im Rahmen von NetApp Backup and Recovery.
- **Backup und Recovery Restore-Administrator**: Workloads mit NetApp Backup and Recovery wiederherstellen.
- **Backup and Recovery Klonadministrator**: Anwendungen und Daten mit NetApp Backup and Recovery klonen.
- **Backup and Recovery-Anzeige**: Informationen in NetApp Backup and Recovery anzeigen, aber keine Aktionen ausführen.

Einzelheiten zu allen NetApp Console-Zugriffsrollen finden sich unter "die Dokumentation zur Einrichtung und Administration der Konsole".

Rollen für gängige Aktionen

Die folgende Tabelle zeigt die Aktionen, die jede NetApp Backup and Recovery-Rolle für alle Workloads ausführen kann.

Funktion und Aktion	Backup und Recovery Superadministrator	Backup und Recovery Backup-Administrator	Backup und Recovery Restore-Administrator	Backup and Recovery Klonadministrator	Backup und Recovery-Anzeige
Hosts hinzufügen, bearbeiten oder löschen	Ja	Nein	Nein	Nein	Nein
Plugins installieren	Ja	Nein	Nein	Nein	Nein
Anmeldeinformationen hinzufügen (Host, Instanz, vCenter)	Ja	Nein	Nein	Nein	Nein
Dashboard und alle Registerkarten anzeigen	Ja	Ja	Ja	Ja	Ja
Kostenlose Testversion starten	Ja	Nein	Nein	Nein	Nein
Arbeitslasten ermitteln	Nein	Ja	Ja	Ja	Nein
Lizenzinformationen anzeigen	Ja	Ja	Ja	Ja	Ja
Lizenz aktivieren	Ja	Nein	Nein	Nein	Nein
Hosts anzeigen	Ja	Ja	Ja	Ja	Ja
Zeitpläne:					
Zeitpläne aktivieren	Ja	Ja	Ja	Ja	Nein
Zeitpläne aussetzen	Ja	Ja	Ja	Ja	Nein
Richtlinien und Schutz:					
Schutzpläne anzeigen	Ja	Ja	Ja	Ja	Ja
Schutzpläne erstellen, ändern oder löschen	Ja	Ja	Nein	Nein	Nein
Workloads wiederherstellen	Ja	Nein	Ja	Nein	Nein

Funktion und Aktion	Backup und Recovery Superadministrator	Backup und Recovery Backup-Administrator	Backup und Recovery Restore-Administrator	Backup and Recovery Klonadministrator	Backup und Recovery-Anzeige
Klone erstellen, aufteilen oder löschen	Ja	Nein	Nein	Ja	Nein
Richtlinie erstellen, ändern oder löschen	Ja	Ja	Nein	Nein	Nein
Berichte:					
Berichte anzeigen	Ja	Ja	Ja	Ja	Ja
Berichte erstellen	Ja	Ja	Ja	Ja	Nein
Berichte löschen	Ja	Nein	Nein	Nein	Nein
Vom SnapCenter Host importieren und Host verwalten:					
Importierte SnapCenter-Daten anzeigen	Ja	Ja	Ja	Ja	Ja
Daten aus SnapCenter importieren	Ja	Ja	Nein	Nein	Nein
Host verwalten (migrieren)	Ja	Ja	Nein	Nein	Nein
Einstellungen konfigurieren:					
Protokollverzeichnis konfigurieren	Ja	Ja	Ja	Nein	Nein
Instanzanmeldeinformationen zuordnen oder entfernen	Ja	Ja	Ja	Nein	Nein
Buckets:					
Buckets anzeigen	Ja	Ja	Ja	Ja	Ja
Bucket erstellen, bearbeiten oder löschen	Ja	Ja	Nein	Nein	Nein

Rollen, die für arbeitslastspezifische Aktionen verwendet werden

Die folgende Tabelle zeigt die Aktionen, die jede NetApp Backup and Recovery Rolle für bestimmte Arbeitslasten ausführen kann.

Kubernetes-Workloads

Diese Tabelle zeigt die Aktionen an, die jede NetApp Backup and Recovery-Rolle für Aktionen speziell für Kubernetes-Workloads durchführen kann.

Funktion und Aktion	Backup und Recovery Superadministrator	Backup und Recovery Backup-Administrator	Backup und Recovery Restore-Administrator	Backup und Recovery-Anzeige
Cluster, Namensräume, Speicherklassen und API-Ressourcen	Ja	Ja	Ja	Ja
Neue Kubernetes Cluster hinzufügen	Ja	Ja	Nein	Nein
Clusterkonfigurationen aktualisieren	Ja	Nein	Nein	Nein
Cluster aus der Verwaltung entfernen	Ja	Nein	Nein	Nein
Anwendungen anzeigen	Ja	Ja	Ja	Ja
Neue Anwendungen erstellen und definieren	Ja	Ja	Nein	Nein
Anwendungskonfigurationen aktualisieren	Ja	Ja	Nein	Nein
Anwendungen aus der Verwaltung entfernen	Ja	Ja	Nein	Nein
Geschützte Ressourcen und Sicherungsstatus anzeigen	Ja	Ja	Ja	Ja
Backups erstellen und Anwendungen mit Richtlinien schützen	Ja	Ja	Nein	Nein
Apps aufheben und Backups löschen	Ja	Ja	Nein	Nein
Wiederherstellungspunkte und Ergebnisse der Ressourcenanzeige	Ja	Ja	Ja	Ja
Anwendungen aus Wiederherstellungspunkten wiederherstellen	Ja	Nein	Ja	Nein
Kubernetes Backup-Richtlinien anzeigen	Ja	Ja	Ja	Ja
Kubernetes Backup-Richtlinien erstellen	Ja	Ja	Ja	Nein

Funktion und Aktion	Backup und Recovery Superadministrator	Backup und Recovery Backup-Administrator	Backup und Recovery Restore-Administrator	Backup und Recovery-Anzeige
Backup-Richtlinien aktualisieren	Ja	Ja	Ja	Nein
Sicherungsrichtlinien löschen	Ja	Ja	Ja	Nein
Ausführungshooks und Hook-Quellen anzeigen	Ja	Ja	Ja	Ja
Ausführungshooks und Hook-Quellen erstellen	Ja	Ja	Ja	Nein
Ausführungshooks und Hook-Quellen aktualisieren	Ja	Ja	Ja	Nein
Ausführungshooks und Hook-Quellen löschen	Ja	Ja	Ja	Nein
Ausführungshook-Vorlagen anzeigen	Ja	Ja	Ja	Ja
Vorlagen für Ausführungs-Hooks erstellen	Ja	Ja	Ja	Nein
Aktualisierung der Ausführungshook-Vorlagen	Ja	Ja	Ja	Nein
Ausführungshook-Vorlagen löschen	Ja	Ja	Ja	Nein
Übersicht der Arbeitslast und Analyse-Dashboards	Ja	Ja	Ja	Ja
StorageGRID Buckets und Speicherziele anzeigen	Ja	Ja	Ja	Ja

Konsolenintegrationen und Dienste konfigurieren

Lokale Bereitstellung der NetApp Console in Active Directory integrieren

Die lokale NetApp Console-Bereitstellung kann mit Active Directory für verzeichnisgestützte Anmeldung und Benutzersuche integriert werden. Der Verzeichnisdienst authentifiziert die Benutzer, anschließend wird diesen Benutzern in der lokalen NetApp Console-Bereitstellung Zugriff zugewiesen.

Erforderliche Zugriffsrollen

Super Admin oder Organisationsadministrator. "Informationen zu Zugriffsrollen".

Bei der Integration mit Active Directory authentifiziert die lokale Bereitstellung von Console die Benutzer über Ihr bestehendes Verzeichnis. Nachdem ein Verzeichnisbenutzer hinzugefügt wurde, können Console Zugriffsrollen zugewiesen werden, um zu steuern, worauf dieser Benutzer zugreifen kann.

Die Active Directory Integration unterstützt zudem die Erfüllung von Compliance-Anforderungen, indem bestehende Kontrollen, Audit-Trails und Richtlinien auf den lokalen NetApp Console-Bereitstellungszugriff angewendet werden.

- Die Active Directory Integration erstellt keine föderierten Gruppen, synchronisiert keine Verzeichnisgruppen-Zuordnungen und gewährt keinen automatischen Zugriff. Administratoren fügen weiterhin Verzeichnisbenutzer zur Organisation hinzu und weisen Rollen in der lokalen Console-Bereitstellung zu.
- Es wird jeweils nur eine Active Directory Integration unterstützt. Sobald eine Integration konfiguriert ist, ist die Schaltfläche **Integration hinzufügen** deaktiviert. Um zu einem anderen Verzeichnis zu wechseln, muss zunächst die bestehende Integration deaktiviert oder gelöscht werden.
- Verzeichnisbenutzer konfigurieren oder verwenden keine Multi-Faktor Authentifizierung (MFA). Die lokale Konsolenbereitstellung unterstützt MFA nur für lokale Benutzer. "Informationen zur Verwaltung der Sicherheitseinstellungen für Mitglieder".

Bevor Sie beginnen

Bevor Sie die Integration mit Active Directory vornehmen, vergewissern Sie sich, dass Sie Folgendes haben:

- Eine Active Directory Domain und Anmeldeinformationen, die das Verzeichnis abfragen können
- Die LDAP-Serveradresse und der Basis individueller Name (DN) für den Verzeichnisbaum
- Netzwerkzugriff von der lokalen NetApp Console-Bereitstellung auf Ihren LDAP-Server über Port 389 (LDAP) oder 636 (LDAPS)
- SSL/TLS-Zertifikate, wenn die Verwendung von LDAPS vorgesehen ist

Schritte

1. **Verwaltung > Identität und Zugriff** auswählen.
2. **Verzeichnisdienste** auswählen, um die Seite „Verbände“ zu öffnen.
3. **Integration hinzufügen** auswählen.
4. Geben Sie die Verbindungsdetails für Ihren Active Directory Server ein:
   - Ein beschreibender Name für die Integration.
   - Der **LDAP-Host**: Hostname oder IP-Adresse Ihres LDAP-Servers. Bei mehreren Servern den primären angeben.
   - Der Port: 389 für LDAP oder 636 für LDAPS.
   - Die **Verbindungs-Zeitüberschreitung** in Millisekunden. Der Standardwert beträgt 1000 ms.
5. **SSL/TLS verwenden** auswählen, um LDAPS zu nutzen. Es sollte bestätigt werden, dass der LDAP-Server LDAPS unterstützt und dass die Konsole auf die erforderlichen Zertifikate zugreifen kann.
6. Die Verbindung testen. Falls diese fehlschlägt, den LDAP-Host, den Port, die Netzwerkverbindung und die SSL/TLS-Zertifikate überprüfen.
7. Nach erfolgreichem Test sind das Verzeichnis und die Benutzerdaten einzugeben:
   - **Base DN-Bindung**: Geben Sie den Bind DN für das LDAP/AD-Konto ein, das diese Anwendung für die

Verbindung zum Verzeichnis verwendet, und geben Sie die Bind-Anmeldeinformationen (Passwort) für dieses Konto ein. Die Console verwendet diese Angaben, um eine Verbindung zu LDAP herzustellen und die Verbindung zu validieren.

- **Benutzer-DN**: Ein Benutzerkonto mit der Berechtigung, das Verzeichnis abzufragen. Zum Beispiel `CN=ldap-reader,OU=Service Accounts,DC=example,DC=com`.

8. **Hinzufügen** auswählen, um die Integration zu speichern.

Nachdem Sie fertig sind

Nachdem die Integration gespeichert wurde, können Verzeichnisbenutzer zur Organisation hinzugefügt und Rollen zugewiesen werden. Mindestens eine Active Directory Integration muss konfiguriert und aktiviert sein, bevor Verzeichnisbenutzer hinzugefügt werden können. "Informationen zum Hinzufügen von Verzeichnisbenutzern und zum Zuweisen von Rollen".

Eine Active Directory Integration deaktivieren oder aktivieren

Eine Integration kann deaktiviert werden, um die verzeichnisbasierte Authentifizierung vorübergehend auszusetzen, ohne die Konfiguration zu löschen. Wenn ein Verzeichnisdienst deaktiviert ist, können sich Verzeichnisbenutzer nicht über das Verzeichnis anmelden.

Schritte

1. **Verwaltung > Identität und Zugriff** auswählen.
2. **Verzeichnisdienste** auswählen, um die Seite „Verbände“ zu öffnen.
3. In der Integrationsliste die Integration suchen und das Aktionsmenü für diese Zeile auswählen.
4. **Deaktivieren** setzt die Integration aus, **Aktivieren** stellt sie wieder her.

Eine Active Directory Integration löschen

Durch das Löschen einer Integration wird die Verzeichnisdienstkonfiguration dauerhaft entfernt. Vor dem Löschen sind alle Warnungen zu den mit der Integration verknüpften Verzeichnisbenutzern zu prüfen, da deren Zugriff beeinträchtigt wird.

Schritte

1. **Verwaltung > Identität und Zugriff** auswählen.
2. **Verzeichnisdienste** auswählen, um die Seite „Verbände“ zu öffnen.
3. In der Integrationsliste die Integration suchen und das Aktionsmenü für diese Zeile auswählen.
4. **Löschen** auswählen und die Löschung bestätigen.

LLM verbinden und den NetApp Console Assistenten in der NetApp Console lokalen Bereitstellung aktivieren

Verbinden Sie Ihr großes Sprachmodell (LLM) mit der lokalen NetApp Console-Bereitstellung, um den Console-Assistenten und die KI-gestützte Speicherverwaltung zu aktivieren.

Diese Dokumentation zur Verbindung eines LLM mit dem Konsolenassistenten zur Aktivierung von KI-Funktionen wird als Technologievorschau bereitgestellt. Mit diesem Vorschauangebot behält sich NetApp das Recht vor, Angebotsdetails, Inhalte und Zeitplan vor der allgemeinen Verfügbarkeit zu ändern.

Erforderliche Zugriffsrollen

Super Admin oder Organisationsadministrator. "Informationen zu Zugriffsrollen".

Nach der Einrichtung öffnen die Benutzer den Konsolenassistenten über das Dashboard und wählen einen Zugriffsmodus aus:

- Im **Nur-Lese-Modus** beantwortet der Assistent Fragen und gibt Hilfestellungen, ohne Änderungen vorzunehmen.
- Im **Lese/Schreib**-Modus kann der Assistent auf die Speicherinfrastruktur zugreifen. Vor jeder Änderung werden Details zur Überprüfung und Bestätigung angezeigt. Für asynchrone Vorgänge, wie die Volume-Erstellung, wird ein Auftrag erstellt, den Benutzer über den Assistenten einsehen können.

Um Ihr LLM zu verbinden, einen Anbieterpfad auswählen, Endpunktdetails und API-Schlüssel eingeben und anschließend ein Modell unter **Administration > AI Tools** auswählen. Assistentenaktionen bleiben innerhalb Ihrer Speicherrichtlinien und rollenbasierten Zugriffskontrollen.

Sammeln Sie alles Notwendige, bevor Sie eine Verbindung zu einem LLM herstellen.

Bevor Sie Ihr LLM verbinden, sollten Sie Folgendes bereithalten:

- Ihre Entscheidung für einen Anbietertyp: OpenAI oder OpenAI-kompatibel. "Informationen zu den verfügbaren Anbieteroptionen."
- Ein gültiger API-Schlüssel für den ausgewählten Anbieterpfad.
- Die Endpunkt-URL für Ihren Anbieterpfad.
- Ihre Proxy- oder Gateway-URL, falls Ihre Organisation eine benötigt.
- Ihr Benutzername oder Ihre Single Sign-On (SSO)-ID für das LLM-Anbieterkonto, falls erforderlich.
- Netzwerkzugriff von der lokalen NetApp Console-Bereitstellung zum ausgewählten Endpunkt.
- Speicherklassen und rollenbasierte Zugriffskontrollen für die Assistentenaktionen, die Sie zulassen möchten.

Details zu den unterstützten Modellen sind unter "Informationen zu unterstützten LLM-Anbietern und Modellen in der lokalen NetApp Console-Bereitstellung" zu finden.

Eine LLM mit einer lokalen NetApp Console-Bereitstellung verbinden

Anbietereinstellungen, API-Schlüssel und Modell eingeben, um Ihre LLM mit der lokalen NetApp Console-Bereitstellung zu verbinden.

Schritte

1. Anmeldung bei der lokalen NetApp Console-Bereitstellung.
2. **Administration > AI Tools** auswählen.
3. Das Menü auswählen und anschließend **Bearbeiten** wählen.
4. Unter **Anbietertyp** einen Anbietertyp auswählen.

   "Informationen zur LLM-Integration in der lokalen NetApp Console-Bereitstellung".

5. Wenn Sie nach einem Provider-Endpunkt gefragt werden, die Endpunkt-URL für den ausgewählten Provider-Pfad eingeben.
6. Geben Sie die Proxy- oder Gateway-URL und die Zugangsdaten ein.

7. Im Feld **Benutzername** ist Ihr Benutzername oder Ihre SSO-ID einzugeben, wenn Ihr Providerpfad dies erfordert.
8. Im Feld **API-Schlüssel** den API-Schlüssel aus dem Pfad des ausgewählten Anbieters einfügen.
9. Ein Modell aus der Liste auswählen.
10. Die Konfiguration kann überprüft und anschließend **Speichern** ausgewählt werden.

    Falls das Speichern oder Testen fehlschlägt, sollten der Anbietertyp, die Endpunkt-URL, der API-Schlüssel und das ausgewählte Modell überprüft und anschließend ein erneuter Versuch unternommen werden.

"Fehlerbehebung bei Ihrer LLM-Integration".

Es wird überprüft, ob die LLM Integration funktioniert.

Nachdem die Konfiguration gespeichert wurde, lassen sich die Verfügbarkeit und das Verhalten des Assistenten überprüfen.

Schritte

1. Bestätigt wird, dass die Schaltfläche **Konsolenassistent** auf dem NetApp Console Dashboard für die lokale Bereitstellung angezeigt wird.
2. Den Assistenten im **Nur-Lese-Modus** öffnen und eine einfache Abfrage ausführen.
3. Den Assistenten im **Lese-/Schreibmodus** öffnen und bestätigen, dass speicherverändernde Aktionen vor der Ausführung eine Benutzerbestätigung erfordern.
4. Es sollte überprüft werden, dass die Benutzer, die Aktionsworkflows benötigen, über die erforderlichen rollenbasierten Zugriffskontrollen verfügen.

Nach Abschluss der Validierung können Benutzer den Konsolenassistenten über das Dashboard öffnen und Aufgaben in einfacher Sprache beschreiben. Beispiele für die Nutzung und Endbenutzer-Workflows finden sich unter "Den NetApp Console Assistenten verwenden".

Zugangsdaten schützen und LLM-Nutzung überwachen

- Nach Möglichkeit sollte ein dedizierter API-Schlüssel für die lokale Bereitstellungsintegration der Konsole verwendet werden.
- API-Schlüssel werden gemäß den Richtlinien Ihrer Organisation rotiert.
- Der Zugriff auf die Einstellungen der KI-Tools ist ausschließlich auf die erforderlichen Administratorrollen beschränkt.
- Die API-Nutzung und Warnmeldungen auf Anbieterseite werden überwacht, um ungewöhnliche Aktivitäten oder Kostenspitzen nachzuverfolgen.

Fehlerbehebung bei der LLM-Integration in der lokalen NetApp Console-Bereitstellung

Mit diesem Schnelltest lassen sich häufige LLM-Integrationsprobleme in der lokalen NetApp Console-Bereitstellung diagnostizieren und beheben.

Diese Dokumentation zur Verbindung eines LLM mit dem Konsolenassistenten zur Aktivierung von KI-Funktionen wird als Technologievorschau bereitgestellt. Mit diesem Vorschauangebot behält sich NetApp das Recht vor, Angebotsdetails, Inhalte und Zeitplan vor der allgemeinen Verfügbarkeit zu ändern.

Falls die Einrichtung noch nicht abgeschlossen ist, siehe "Verbinden Sie Ihren LLM und aktivieren Sie den NetApp Console Assistenten".

LLM-Integrationsprobleme schnell eingrenzen

1. Die Konfiguration der KI-Tools in **Administration > KI-Tools** kann validiert werden.

   Anbietertyp, Endpunkt-URL, API-Schlüssel, ausgewähltes Modell und ausgehender Netzwerkzugriff werden bestätigt.

2. Die Verfügbarkeit des Assistenten im Dashboard wird angezeigt.

   Bestätigt wird, dass die Schaltfläche **Konsolenassistent** für die erwarteten Benutzer und Organisationen erscheint.

3. Laufzeitverhalten überprüfen.

   Eine einfache Leseanfrage ausführen und die Erreichbarkeit des Provider-Endpunkts, die Verfügbarkeit des Modells sowie den Zustand des Provider-Dienstes bestätigen.

Fehlerbehebung anhand der Symptome

Symptom	Wahrscheinliche Ursache	Was überprüft werden sollte	Nächster Schritt
Speichern oder Testen schlägt in AI Tools fehl	Konfigurations- oder Verbindungsinkonsistenz	Anbietertyp, Endpunkt-URL, API-Schlüsselformat, ausgewähltes Modell und ausgehender Zugriff	Der Wert, der die Validierung nicht besteht, muss korrigiert und erneut gespeichert werden.
Die Schaltfläche „Console assistant“ fehlt.	Unzureichender Integrationsstatus, Organisationskonflikt oder RBAC-Konflikt	Erfolgreiche Speicherung von KI-Tools, Integrationsstatus, aktuelle Organisation und erwartete Zugriffsrolle	Die Sitzung wird aktualisiert und mit einem bekannten, funktionierenden Administratorkonto überprüft.
Assistent öffnet sich, aber die Anfrage schlägt fehl	Problem mit dem Anbieter oder dem Laufzeitpfad	Erreichbarkeit des Endpunkts, Modellverfügbarkeit auf diesem Endpunkt, Anbieterlimits und temporärer Anbieterstatus	Nach Behebung von Endpunkt-/Modellkonflikten oder Anbieterseitigen Limitproblemen erneut versuchen
Die Antwort des Assistenten ist langsam oder inkonsistent.	Eingabeaufforderungsgröße, Endpunktleistung oder Netzwerk-/Proxy-Instabilität	Kurzer Schnelltest, Verfügbarkeit des Anbieterdienstes und Netzwerk-/Proxy-Stabilität	Eine kürzere Eingabeaufforderung verwenden, ein anderes unterstütztes Modell ausprobieren und das Netzwerk- oder Proxy-Routing stabilisieren

Auf Offenlegung oder Missbrauch von LLM-Anmeldedaten reagieren

Wenn Sie den Verdacht haben, dass der API-Schlüssel offengelegt oder unbefugt verwendet wurde:

1. Der bestehende API-Schlüssel wird im Anbietersystem widerrufen.
2. Einen neuen API-Schlüssel erstellen.
3. Der Schlüssel wird unter **Administration > AI Tools** aktualisiert.

4. Die erfolgreiche Wiederverbindung mit einem schreibgeschützten Assistententest wird überprüft.

Benachrichtigungszustellungskanäle in der lokalen NetApp Console-Bereitstellung einrichten

In der lokalen NetApp Console-Bereitstellung können mehrere Kanäle für Benachrichtigungen eingerichtet werden, darunter E-Mail und Webhooks.

Erforderliche Zugriffsrollen

Super Admin oder Organisationsadministrator. "Informationen zu Zugriffsrollen".

Standardmäßig werden Benachrichtigungen bei der lokalen Bereitstellung der Console über das integrierte Benachrichtigungssystem angezeigt. Die Konfiguration zusätzlicher Zustellungskanäle ermöglicht den Empfang von Benachrichtigungen auf die Weise, die am besten zum eigenen Workflow passt.

Sie können alle Benachrichtigungen über dieselben Kanäle versenden oder für verschiedene Benachrichtigungstypen unterschiedliche Kanäle verwenden. Beispielsweise können dringende Speicherwarnungen per E-Mail versendet werden, während anderer Alarmverkehr über einen Webhook an ein externes Überwachungstool weitergeleitet wird.

Nachdem Benachrichtigungskanäle eingerichtet wurden, lassen sich Benachrichtigungsregeln konfigurieren und verschiedenen Kanälen zuweisen. "Informationen zur Konfiguration von Benachrichtigungsregeln".

E-Mail-Server konfigurieren

Wenn ein E-Mail-Server konfiguriert ist, sendet Console local deployment Benachrichtigungen, Warnungen und Benutzereinladungen darüber. Console local deployment unterstützt SMTP-E-Mail-Server, die entweder Ihr bestehender Unternehmens-E-Mail-Server oder ein E-Mail-Dienst eines Drittanbieters sein können.

Schritte

1. **Administration > Konsole** auswählen.
2. **Konfiguration** öffnet die Seite „Systemkonfigurationen“.
3. Im Abschnitt **E-Mail-Server** auf **Konfigurieren** auswählen.
4. Geben Sie die Verbindungsdetails für Ihren E-Mail-Server ein:
   - Einen Absendernamen und eine Absender-E-Mail-Adresse hinzufügen.
   - Der **SMTP-Host**: Hostname oder IP-Adresse Ihres SMTP-Servers. Bei mehreren Servern ist der primäre anzugeben.
   - Wählen Sie das Verbindungsprotokoll aus der Dropdown-Liste **Verbindungssicherheit** aus. Der Port ist vorkonfiguriert und schreibgeschützt: 25 für SMTP mit STARTTLS oder 465 für SMTPS.

     SMTPS (Port 465) stellt sofort eine verschlüsselte Verbindung her und wird für sicherheitskritische Umgebungen empfohlen. STARTTLS (Port 25) wertet eine unverschlüsselte Verbindung auf und kann auf unverschlüsselte Übertragung zurückgreifen, falls die Verschlüsselungsaushandlung fehlschlägt.
5. **Test-E-Mail** auswählen, um eine Test-E-Mail an einen angegebenen Empfänger zu senden.
6. Nach erfolgreichem Test **Speichern** auswählen, um die Konfiguration zu speichern.

   Falls der Test fehlschlägt, sollten die eingegebenen Einstellungen erneut überprüft und zusätzlich sichergestellt werden, dass die lokale Console-Bereitstellung Netzwerkzugriff auf den E-Mail-Server hat.

Aktualisierung einer E-Mail-Server-Konfiguration

Sie können eine bestehende E-Mail-Server-Konfiguration aktualisieren, wenn Sie einen anderen E-Mail-Server verwenden möchten.

Schritte

1. **Administration > Konsole** auswählen.
2. **Konfiguration** öffnet die Seite „Systemkonfigurationen“.
3. Im Abschnitt **E-Mail-Server** auf **Konfigurieren** auswählen.
4. **Felder löschen** auswählen, um die bestehende Konfiguration zu löschen.
5. Geben Sie die neuen Verbindungsdaten für Ihren E-Mail-Server ein.
6. **Test-E-Mail** auswählen, um eine Test-E-Mail an einen angegebenen Empfänger zu senden.
7. Nach erfolgreichem Test auf **Speichern** auswählen, um die neue Konfiguration zu speichern.

   Falls der Test fehlschlägt, sollten die eingegebenen Einstellungen erneut überprüft und zusätzlich sichergestellt werden, dass die lokale Console-Bereitstellung Netzwerkzugriff auf den E-Mail-Server hat.

Eine E-Mail-Serverkonfiguration entfernen

Sie können die E-Mail-Server-Konfiguration entfernen, wenn Sie nicht mehr möchten, dass die lokale Console Bereitstellung E-Mails versendet.

Schritte

1. **Administration > Konsole** auswählen.
2. **Konfiguration** auswählen, um die Seite Systemkonfiguration zu öffnen.
3. Im Abschnitt **E-Mail-Server** auf **Konfigurieren** auswählen.
4. **Felder löschen** auswählen, um die bestehende Konfiguration zu löschen.
5. **Speichern** auswählen, um die gelöschte Konfiguration zu speichern, wodurch die E-Mail-Server-Konfiguration aus der Console lokalen Bereitstellung entfernt wird.

Einen Webhook konfigurieren

Webhooks können eingerichtet werden, um Benachrichtigungen von der lokalen Console Bereitstellung an andere Tools oder Dienste zu senden. Es ist möglich, mehrere Webhooks zu konfigurieren, die jeweils auf einen anderen Endpunkt verweisen. Zum Beispiel einen für ein SIEM und einen weiteren für einen On-Call-Paging-Dienst.

Nachdem ein Webhook erstellt wurde, können Benutzer mit der Rolle Storage admin diesen bestimmten Alarmregeln zuweisen. Beispielsweise ist es möglich, kritische Alarme per E-Mail zu versenden, während alle Alarme über einen Webhook an ein Drittanbieter-Überwachungstool weitergeleitet werden.

Bei der lokalen Bereitstellung über die Konsole wird keine Zugriffskontrolle für Webhook-Endpunkte erzwungen. Jeder Benutzer oder jedes System, das die Endpunkt-URL erreichen kann, erhält die Alarmdaten. Es sollte sichergestellt sein, dass der Zugriff auf die empfangende Anwendung durch die Zugriffskontrollen dieser Anwendung auf autorisierte Benutzer beschränkt ist.

Bevor Sie beginnen

Es sollte bestätigt werden, dass die lokale Console-Bereitstellung die empfangende Anwendung über das

Netzwerk erreichen kann, und die Endpunkt-URL, die HTTP-Methode sowie alle von dieser Anwendung benötigten Authentifizierungs- oder Zertifikatsdetails sollten erfasst werden.

Schritte

1. **Administration > Konsole** auswählen.
2. **Konfiguration** öffnet die Seite „Systemkonfigurationen“.
3. Im Abschnitt **Webhook-Integration** auf **Konfigurieren** auswählen.
4. Geben Sie die erforderlichen Details für den Webhook ein:
   - Ein beschreibender Name für den Webhook.
   - Die von der empfangenden Anwendung bereitgestellte Endpoint-URL.
   - HTTP-Methode
   - Optional: Ein selbstsigniertes Zertifikat im PEM-Format.
   - Alle erforderlichen Header oder Geheimnisse (Authentifizierungsdaten).
   - Das Format, das beim Senden des Webhooks verwendet werden soll. JSON und OTEL (OpenTelemetry) werden unterstützt.

     JSON wird für allgemeine Webhooks und benutzerdefinierte REST-Endpunkte verwendet. OTEL wird für Observability-Plattformen verwendet, die OpenTelemetry-Signale nativ verarbeiten, wie Grafana oder andere OpenTelemetry-kompatible Collector.
5. **Webhook testen** auswählen, um die Webhook-Verbindung zu testen und sicherzustellen, dass die Console lokale Bereitstellung erfolgreich Nachrichten an die empfangende Anwendung senden kann.
6. Nach erfolgreichem Test **Speichern** auswählen, um den Webhook zu erstellen.

   Nach dem Speichern des Webhooks steht er Benutzern zur Auswahl zur Verfügung, wo Webhooks unterstützt werden, wie beispielsweise bei den Optionen zur Benachrichtigungszustellung. "Informationen zum Erstellen von Alarmregeln und zum Zuweisen von Webhooks für die Alarmzustellung."

NetApp Console verwenden

Anmeldung bei der lokalen NetApp Console-Bereitstellung

Sie können sich bei der lokalen NetApp Console-Bereitstellung anmelden, nachdem Ihr Organisationsadministrator Sie zu Ihrem Benutzerkonto für die lokale Console-Bereitstellung eingeladen hat. Für die Anmeldung wird die mit Ihrem Login verknüpfte E-Mail-Adresse verwendet.

Wenn Sie sich anmelden, aber keine Ressourcen sehen, wenden Sie sich an Ihren Organisationsadministrator. "Wenden Sie sich an Ihren Organisationsadministrator".

Schritte

1. Einen Webbrowser öffnen und zur IP-Adresse wechseln, an der die lokale Console-Bereitstellung installiert ist.
2. Auf der **Anmeldeseite** die E-Mail-Adresse eingeben, die mit Ihrem Login verknüpft ist.
3. Je nach dem mit Ihrer Anmeldung verknüpften Authentifizierungsverfahren werden Sie zur Eingabe Ihrer Anmeldedaten aufgefordert.

- Ein NetApp Console Konto mit Ihrer E-Mail-Adresse und einem Passwort

  - Wenn die Multi-Faktor-Authentifizierung (MFA) aktiviert ist: Nach Eingabe Ihres Passworts werden Sie aufgefordert, einen TOTP-Code (aus Ihrer Authentifizierungs-App) einzugeben oder einen Wiederherstellungscode zu verwenden.
  - Wenn Sie sich mit Wiederherstellungscodes anmelden, verwenden Sie diese in der Reihenfolge, die in der Benutzeroberfläche während der Wiederherstellungscode-Aufforderung angezeigt wird.

+

- Ein Active Directory Konto mit Ihrer E-Mail-Adresse und Ihrem Passwort

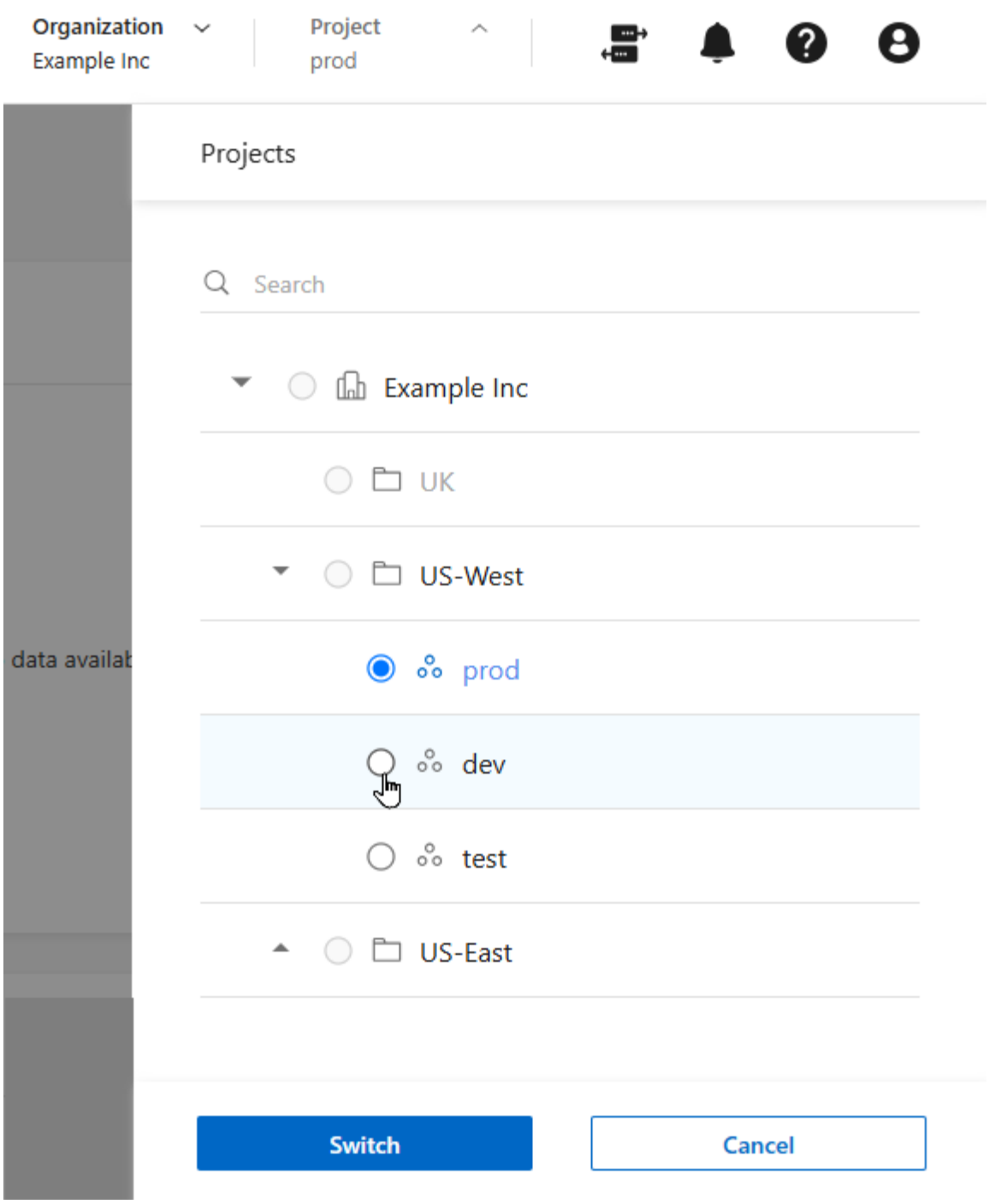
Zwischen Flotten in der lokalen Bereitstellung der NetApp Console wechseln

In der lokalen NetApp Console-Bereitstellung kann jederzeit zwischen mehreren Flotten gewechselt werden, sofern Zugriff auf diese besteht.

Sie können nicht zu einer anderen Flotte wechseln, während Sie eine der **Identitäts- und Zugriffs**-Seiten anzeigen.

Schritte

1. Im oberen Bereich der lokalen NetApp Console-Bereitstellung wird **Bereich** ausgewählt.
2. Durchsuchen Sie die Flotten in Ihrer Organisation, wählen Sie die gewünschte Flotte aus und wählen Sie dann **Wechseln**.



Verwaltung der Benutzereinstellungen Ihrer lokalen NetApp Console-Bereitstellung

In der lokalen NetApp Console-Bereitstellung kann das lokale Console-Bereitstellungsprofil geändert werden, einschließlich der Änderung des Passworts, der Aktivierung der Multi-Faktor-Authentifizierung (MFA) und der Anzeige, wer der Console-Administrator ist.

Anzeigename ändern

Sie können Ihren lokalen Anzeigenamen für die Console-Bereitstellung ändern, der Sie für andere Benutzer

identifiziert. Ihr Benutzername und Ihre E-Mail-Adresse können nicht geändert werden.

Schritte

1. Das Profilsymbol in der oberen rechten Ecke der lokalen Konsolenbereitstellung öffnet das Benutzereinstellungsfeld.
2. Das Symbol **Bearbeiten** neben Ihrem Namen auswählen.
3. Geben Sie Ihren neuen Anzeigenamen im Feld **Name** ein.

Multifaktor-Authentifizierung konfigurieren

Die Multi-Faktor-Authentifizierung (MFA) kann konfiguriert werden, um die Sicherheit zu erhöhen, indem beim Anmelden an der lokalen NetAppConsole-Bereitstellung eine zweite Verifizierungsmethode erforderlich ist.

Nutzer, die sich über die NetApp Support Site anmelden, können MFA nicht aktivieren. Wenn dies auf Sie zutrifft, wird die Option zur Aktivierung von MFA in Ihren Profileinstellungen nicht angezeigt.

Die Multi-Faktor-Authentifizierung sollte nicht aktiviert werden, wenn Ihr Benutzerkonto für den API-Zugriff verwendet wird. Multi-Faktor-Authentifizierung verhindert den API-Zugriff, wenn sie für ein Benutzerkonto aktiviert ist. Für den gesamten API-Zugriff sind Dienstkonten zu verwenden.

Sie können MFA für Ihr Konto nicht über die lokale Bereitstellung der Konsole konfigurieren, wenn Ihr Konto Active Directory oder einen anderen integrierten Verzeichnisdienst für die Authentifizierung verwendet.

Bevor Sie beginnen

- Sie müssen bereits eine Authentifizierungs-App, wie Google Authenticator oder Microsoft Authenticator, auf Ihr Gerät heruntergeladen haben.
- Sie benötigen Ihr Passwort, um die Multi-Faktor-Authentifizierung einzurichten.

Wenn Sie keinen Zugriff auf Ihre Authentifizierungs-App haben oder Ihren Wiederherstellungscode verlieren, kann Ihr NetApp Console-Administrator Unterstützung bieten.

Schritte

1. Das Profilsymbol in der oberen rechten Ecke der Konsole zeigt das Benutzereinstellungsfeld an.
2. Neben der Überschrift **Multi-Factor Authentication** die Option **Configure** auswählen.
3. Folgen Sie den Anweisungen, um die Multi-Faktor-Authentifizierung für Ihr Konto einzurichten.
4. Nach Abschluss des Vorgangs werden Sie aufgefordert, Ihre Wiederherstellungscodes zu speichern. Es besteht die Möglichkeit, die Codes entweder zu kopieren oder eine Textdatei mit den Codes herunterzuladen. Diese Codes sollten an einem sicheren Ort aufbewahrt werden. Die Wiederherstellungscodes werden benötigt, falls der Zugriff auf die Authentifizierungs-App verloren geht.

   Falls Sie sich mit einem Wiederherstellungscode anmelden müssen, verwenden Sie diese in der Reihenfolge, die in der Benutzeroberfläche während der Aufforderung zur Eingabe des Wiederherstellungscodes angezeigt wird.

   Nachdem Sie die Multi-Faktor-Authentifizierung (MFA) eingerichtet haben, fordert die lokale NetApp Console-Bereitstellung Sie bei jeder Anmeldung auf, einen Einmalcode aus Ihrer Authentifizierungs-App einzugeben.

Ihren MFA-Wiederherstellungscode neu generieren

Ein Wiederherstellungscode kann nur einmal verwendet werden. Wenn Sie Ihren verlieren, erstellen Sie einen neuen.

Schritte

1. Das Profilsymbol in der oberen rechten Ecke der lokalen NetApp Console-Bereitstellung zeigt das Benutzereinstellungsfeld an.
2. Wählen Sie ••• neben der Überschrift **Multi-Faktor-Authentifizierung** aus.
3. **Wiederherstellungscode neu generieren** auswählen.
4. Kopieren Sie die generierten Wiederherstellungscodes und speichern Sie sie an einem sicheren Ort.

Ihre MFA Konfiguration löschen

Durch das Löschen der Multi-Faktor-Authentifizierung (MFA) entfällt der zweite Verifizierungsschritt bei Ihrer nächsten Anmeldung. Um MFA erneut zu verwenden, muss sie in Ihren Benutzereinstellungen erneut konfiguriert werden.

Falls Sie nicht auf Ihre Authentifizierungs-App oder Ihren Wiederherstellungscode zugreifen können, ist eine Kontaktaufnahme mit Ihrem Organisationsadministrator erforderlich, um Ihre MFA Konfiguration zurückzusetzen.

Schritte

1. Das Profilsymbol in der oberen rechten Ecke der lokalen Konsolenbereitstellung öffnet das Benutzereinstellungsfeld.
2. Wählen Sie ••• neben der Überschrift **Multi-Faktor-Authentifizierung** aus.
3. Wählen Sie **Delete**.

Wenden Sie sich an Ihren Organisationsadministrator

Wenn Sie den Administrator Ihrer Organisation kontaktieren müssen, können Sie ihm direkt aus der Console eine E-Mail senden. Der Administrator verwaltet die Benutzerkonten und Berechtigungen innerhalb Ihrer Organisation.

Für die Nutzung der Funktion **Administratoren kontaktieren** muss für Ihren Browser eine Standard-E-Mail-Anwendung konfiguriert sein.

Schritte

1. Das Profilsymbol in der oberen rechten Ecke der lokalen Konsolenbereitstellung öffnet das Benutzereinstellungsfeld.
2. **Administratoren kontaktieren** auswählen, um eine E-Mail an den Administrator Ihrer Organisation zu senden.
3. Die zu verwendende E-Mail-Anwendung auswählen.
4. Die E-Mail fertigstellen und **Senden** auswählen.

Dunkelmodus konfigurieren (dunkles Design)

Die lokale NetApp Console-Bereitstellung kann im Dunkelmodus angezeigt werden.

Schritte

1. Das Profilsymbol in der oberen rechten Ecke der lokalen Konsolenbereitstellung öffnet das Benutzereinstellungsfeld.
2. Den Schieberegler für das **Dark theme** nach rechts bewegen, um es zu aktivieren.

Den NetApp Console-Assistenten in der NetApp Console lokalen Bereitstellung verwenden

Der NetApp Console Assistent in der NetApp Console lokalen Bereitstellung ermöglicht das Verwalten von Speicher und das Erhalten von Antworten in natürlicher Sprache. Bedarf kann in einfacher Sprache beschrieben werden, und die NetApp Console lokale Bereitstellung handelt entsprechend den Speicherrichtlinien und dem rollenbasierten Zugriff.

> Diese Dokumentation zur Verbindung eines LLM mit dem Konsolenassistenten zur Aktivierung von KI-Funktionen wird als Technologievorschau bereitgestellt. Mit diesem Vorschauangebot behält sich NetApp das Recht vor, Angebotsdetails, Inhalte und Zeitplan vor der allgemeinen Verfügbarkeit zu ändern.

Die Aktionen des Assistenten sind durch Ihre zugewiesene rollenbasierte Zugriffsberechtigung eingeschränkt. "Informationen zu Zugriffsrollen".

Erfahren Sie, was mit dem Console Assistent möglich ist

Der Console-Assistent ist eine natürlichsprachliche Schnittstelle zur lokalen NetApp Console-Bereitstellung. Es kann eine Frage gestellt oder eine Aufgabe beschrieben werden, woraufhin eine Antwort oder ein Aktionsvorschlag zurückgegeben wird. Der Assistent bietet folgende Funktionen:

- **Speicher bereitstellen** Eine Arbeitslast wird in einfacher Sprache beschrieben. Der Assistent empfiehlt eine Speicherklasse und einen Speicherort und erstellt anschließend das Volume oder die LUN, nachdem die Details bestätigt wurden. Beispielsweise kann der Assistent aufgefordert werden, ein CIFS-Volume mit einer bestimmten Kapazität zu erstellen. Der Assistent identifiziert den Cluster und die Storage Virtual Machine (SVM), trägt die erforderlichen Parameter ein und stellt den Speicher bereit.
- **Suchen und Hilfe erhalten** Stellen Sie Fragen zu Ihrer Speicherumgebung, finden Sie lokale Bereitstellungsfunktionen der Console und erhalten Sie kontextbezogene Antworten aus der NetApp Dokumentation und dem aktuellen Flottenstatus.
- **Warnungen untersuchen** Der Assistent kann gebeten werden, eine aktive Warnmeldung zu überprüfen. Er analysiert das Problem und schlägt eine Lösung vor oder führt nach Ihrer Bestätigung eine Behebungsmaßnahme durch.

Der Assistent sendet Anfragen ausschließlich an den LLM-Endpunkt, der von Ihrem Administrator in der lokalen Console-Bereitstellung konfiguriert wurde. Vor der Durchführung speicherverändernder Aktionen wird eine Bestätigung angefordert, und alle Aktionen berücksichtigen die Ihrem Konto zugewiesenen rollenbasierten Zugriffskontrollen.

Bestätigen Sie, dass der Konsolenassistent verwendet werden kann.

- Ein Organisationsadministrator oder Superadministrator muss den Konsolenassistenten aktivieren, indem ein großes Sprachmodell (LLM) mit der lokalen Console-Bereitstellung verbunden wird. Wenn die Schaltfläche **Console assistant** im Dashboard nicht angezeigt wird, sollte der Administrator gebeten werden, sie zu aktivieren. Weitere Informationen finden sich unter "Verbinden Sie Ihren LLM und aktivieren

Sie den NetApp Console Assistenten".

- Stellen Sie sicher, dass Sie über die rollenbasierten Zugriffskontrollen verfügen, die für die Aktionen erforderlich sind, die der Assistent ausführen soll.

Dem Konsolenassistenten kann eine Frage gestellt oder eine Aktion angefordert werden.

Den Konsolenassistenten öffnen, einen Zugriffsmodus auswählen und eine Eingabeaufforderung eingeben, die die Anfrage beschreibt.

Schritte

1. Wählen Sie im Dashboard für die lokale Bereitstellung der NetApp Console die Schaltfläche **Console assistant** aus.
2. Zugriffsmodus auswählen:
   - **Nur lesen** ermöglicht es, Fragen zu stellen und Hilfestellung zu erhalten, ohne Änderungen vorzunehmen.
   - **Lesen/Schreiben** auswählen, damit der Assistent auf Ihre Speicherinfrastruktur zugreifen kann.
3. Geben Sie eine Eingabeaufforderung ein, die Ihre Frage oder Aufgabe beschreibt, und wählen Sie dann **Senden**.

   Beispiel: `Create a 10GiB volume for home directories named home, and share it with Everyone set to FULL_CONTROL.`
4. Antwort des Assistenten überprüfen:
   - Für eine Frage gibt der Assistent eine Antwort zurück, auf die Sie reagieren können.
   - Bei einer Aktion zeigt der Assistent die vorgeschlagene Aktion an, fragt nach fehlenden Details wie der Berechtigungsstufe und bittet dann um Bestätigung, bevor er fortfährt.
5. Die Aktion wird bestätigt. Bei asynchronen Vorgängen, wie der Volume-Erstellung, erstellt der Assistent einen Auftrag, um die Anfrage abzuschließen.
6. Um den Status einer Anfrage zu überprüfen, kann der Assistent befragt werden. Beispielsweise kann `Let me know when the job completes` eingegeben werden, woraufhin der Assistent den aktuellen Status zurückmeldet.

Speicher in der NetApp Console verwalten

Informationen zum Flottenmanagement in der lokalen NetApp Console-Bereitstellung

Die Flottenverwaltung in der lokalen NetApp Console-Bereitstellung ist die Praxis, Speichersysteme in logische Gruppen zu organisieren, um einheitliche Richtlinien anzuwenden, den Zugriff zu steuern und den Zustand zusammengehöriger Cluster zu überwachen. Anstatt jeden Cluster unabhängig zu verwalten, ermöglicht die Flottenverwaltung die Behandlung Ihrer Flotte als gemeinsamen Ressourcenpool zur Unterstützung Ihrer Datenspeicherziele.

Mit zunehmender Größe Ihrer Speicherumgebung wird die Verwaltung einzelner Cluster unpraktisch. Flottenmanagement löst dieses Problem, indem eine strukturierte Möglichkeit zur Gruppierung verwandter Systeme, zur Delegation von Verantwortlichkeiten und zur Sicherstellung des Betriebs aller Cluster nach denselben Standards geboten wird.

Warum Flottenmanagement wichtig ist

Das Flottenmanagement befasst sich mit drei zentralen Herausforderungen:

- **Vereinfachung durch Abstraktion** – Flottenmanagement abstrahiert die Komplexität der Verwaltung einzelner Speicherinfrastrukturen. Statt einer Konfiguration von Cluster zu Cluster erfolgt die Verwaltung der gesamten Speicherlandschaft als einheitliches Ganzes, wodurch der operative Aufwand und die Entscheidungsbelastung verringert werden.
- **Konsistenz und Skalierbarkeit** – Ohne klare Organisation treffen verschiedene Teams unterschiedliche Entscheidungen für ähnliche Workloads, was zu fragmentierten Konfigurationen führt. Flottenmanagement ermöglicht die gleichzeitige Anwendung von Standards auf Dutzende von Systemen und stellt so sicher, dass neue Workloads team- und flottenübergreifend auf derselben Basis beginnen.
- **Governance und Kontrolle** – Wenn Teams wachsen, sind klare Zuständigkeiten dafür erforderlich, wer was verwalten kann. Flottenmanagement schafft diese Grenzen durch Organisationsstruktur und Zugriffskontrolle, sodass Speicherentscheidungen weiterhin geregelt und nachvollziehbar bleiben.

Wie Flotten Ihre Ressourcen organisieren

Die Ressourcenhierarchie Ihrer Organisation besteht aus Ordnern und Flotten:

Eine detaillierte Übersicht über die Hierarchie und das Zugriffsmodell befindet sich unter "Informationen zu Ordnern und Flotten in der lokalen Bereitstellung der NetApp Console".

- **Organisation** – Die oberste Ebene, die Ihr Unternehmen repräsentiert.
- **Ordner** – helfen bei der Organisation zusammengehöriger Flotten. Zum Beispiel kann für jede Region oder Geschäftseinheit ein Ordner erstellt und darin Flotten angelegt werden. Ordner können weitere Ordner oder Flotten enthalten. Wird eine Rolle auf Ordnerebene zugewiesen, übernehmen die Mitglieder diese Rolle für alle Flotten innerhalb des Ordners.
- **Flotten** – Die von Ihnen verwalteten Speichersysteme werden gruppiert. Speichersysteme werden Flotten zugeordnet und Mitglieder Flotten zugewiesen, um ihnen Zugriff zu ermöglichen.

> Ordner dienen als Organisationswerkzeug und sind für Mitglieder, die keine IAM-Berechtigungen wie Organization admin, Folder admin oder Fleet admin Rollen besitzen, nicht sichtbar. Mitglieder haben Zugriff auf Flotten, nicht auf Ordner.

Gängige Flottenorganisationsmuster

Die Organisation Ihrer Flotten hängt von Ihrem Betriebsmodell ab:

- **Nach Umgebung** – Separate Flotten für Produktions-, Entwicklungs- und Test-Workloads erstellen. So bleibt der Produktionsspeicher strengeren Richtlinien unterworfen, während in weniger anspruchsvollen Umgebungen mehr Flexibilität möglich ist.
- **Nach Geschäftsbereich** – Cluster, die einer bestimmten Abteilung wie Finanzen, Entwicklung oder Personalwesen dienen, werden zu einer dedizierten Flotte gruppiert. Speicherverwaltungsaufgaben können dann Teammitgliedern innerhalb dieses Geschäftsbereichs zugewiesen werden, ohne dass andere Flotten für sie sichtbar sind.
- **Nach Standort oder Rechenzentrum** - Wenn Cluster über mehrere Standorte verteilt sind, ermöglicht die Organisation nach Standort die Überwachung des Zustands auf Standortebene, die Anwendung regionsspezifischer Richtlinien und die Verfolgung des Kapazitätsverbrauchs pro Standort.
- **Nach Applikations-Tier** – Cluster, die eine bestimmte Klasse von Arbeitslasten hosten, wie Datenbanken, Dateifreigaben oder virtuelle Maschinen, werden gruppiert, sodass einheitliche, auf diesen Arbeitslasttyp

abgestimmte Standards für die gesamte Flotte angewendet werden können.

Ordner können verwendet werden, um eine weitere Organisationsebene hinzuzufügen. Beispielsweise kann für jede Region ein Ordner erstellt und innerhalb jedes regionalen Ordners umgebungsbasierte Flotten angelegt werden.

Wie Flottenmanagement die Zugangskontrolle ermöglicht

Flotten und Ordner dienen als Grenzen für den Benutzerzugriff und die administrative Verantwortung:

- **Zugriff auf Ordnerebene** – Wenn eine Rolle auf Ordnerebene zugewiesen wird, erbt das Mitglied diese Rolle für alle Flotten und Ressourcen innerhalb des Ordners. So ist es möglich, administrative Aufgaben zu delegieren, ohne Zugriff auf die gesamte Organisation zu gewähren.
- **Zugriff auf Flottenebene** - Bei der Zuweisung einer Rolle auf Flottenebene hat das Mitglied nur Zugriff auf die Speichersysteme innerhalb dieser Flotte. Dadurch ist es möglich, die Speicherverwaltung an Teammitglieder oder Anwendungsbesitzer zu delegieren, ohne nicht zugehörige Teile der Infrastruktur offenzulegen.

Die lokale Bereitstellung über die NetApp Console ermöglicht die Überwachung von Zustand und Leistung auf Flottenebene, sodass der Status aller Cluster einer Flotte aus einer einzigen Ansicht ersichtlich ist, Probleme frühzeitig erkannt werden und Maßnahmen ergriffen werden können, bevor sie sich auf die Workloads auswirken.

Wie das Speichermanagement funktioniert

Speichermanagement bezeichnet die Definition von Speicherstandards, deren konsistente Anwendung und den Betrieb von Workloads, sodass deren langfristige Ausrichtung erhalten bleibt. Bei der lokalen Bereitstellung über NetApp Console werden diese Standards in Form von Speicherklassenrichtlinien und Speicherklassen ausgedrückt, die Flotten zugeordnet und durch Bereitstellungs-Workflows durchgesetzt werden, die von RBAC und Audit-Protokollierung gesteuert werden.

Die lokale Bereitstellung über die Konsole verbindet vier Konzepte zu einem einzigen Workflow:

- **Flotten** definieren den Bereich, in dem Sie Speicher verwalten. Eine Flotte gruppiert Systeme, sodass Sie den Zugriff steuern, Standards einheitlich anwenden und Ressourcen als Einheit verwalten können.
- **Speicherklassenrichtlinien** definieren Standards als wiederverwendbare Bausteine (Leistung, Kapazität, Sicherheit, Datenschutz).
- **Speicherklassen** drücken die Absicht bezüglich der Arbeitslast aus. Eine Speicherklasse ist eine benannte Vorlage, die aus einer oder mehreren Richtlinien zusammengesetzt ist.
- **Bereitstellungsworkflows** erstellen Speicher innerhalb festgelegter Grenzen. Unterschiedliche Workflows treffen Konfigurationsentscheidungen auf unterschiedliche Weise, aber alle können Speicherklassen erzwingen und bleiben durch RBAC und Audit-Protokollierung geregelt.

Bereitstellungsansätze

Die lokale Bereitstellung über die Konsole unterstützt drei Bereitstellungsansätze, die alle durch RBAC, Audit-Protokollierung und Speicherklassenstandards geregelt werden:

- **Manuelle Bereitstellung** – Das Zielsystem wird ausgewählt und die Konfigurationsdetails werden direkt angegeben. Diese Option eignet sich, wenn eine explizite Kontrolle über die Systemauswahl und Konfiguration erforderlich ist.
- **Automatisierte Bereitstellung** – Sie geben die Workload-Eingaben an und wählen optional eine Storage-

Klasse aus. Die lokale Bereitstellung über die NetApp Console empfiehlt die optimale Platzierung und wendet klassenbasierte Einstellungen an, um manuelle Entscheidungen zu reduzieren.

- **KI-gestützte (agentenbasierte) Bereitstellung** – Sie beschreiben, was Sie benötigen, in natürlicher Sprache. Die lokale Bereitstellung über die Konsole schlägt einen durch RBAC und Speicherklassen eingeschränkten Plan vor und führt die Bereitstellung erst nach Ihrer Prüfung und Genehmigung durch.

Wie es weitergeht

- Informationen zu Speicherstandards sind unter "Informationen zu Speicherklassen und Richtlinien in der lokalen Bereitstellung der NetApp Console" verfügbar.
- Informationen zum Erstellen und Verwalten von Flotten sind unter "Ordner und Flotten verwalten" verfügbar.
- "Speicher manuell bereitstellen"
- "Speicher automatisch bereitstellen"
- "Speicher mit KI-Unterstützung bereitstellen"

Speicherverhalten standardisieren

Informationen zu Speicherklassen und Richtlinien in der lokalen Bereitstellung der NetApp Console

Eine Speicherklasse ist eine wiederverwendbare Vorlage, die das Verhalten des Speichers definiert. Bei der Bereitstellung von Speicher mithilfe einer Speicherklasse erzwingt die NetApp Console lokale Bereitstellung automatisch die in dieser Klasse kodierten Standards, ohne dass Administratoren für jede Arbeitslast individuelle Konfigurationsentscheidungen treffen müssen.

Speicherklassen basieren auf Speicherklassenrichtlinien, die einzelne Dimensionen des Speicherverhaltens definieren. Zusammen lassen sich die Speicherstandards eines Unternehmens einmalig erfassen und konsistent auf alle Flotten anwenden.

Was Speicherklassenrichtlinien sind

Eine Speicherklassenrichtlinie definiert eine Dimension des Speicherverhaltens. Richtlinien sind wiederverwendbare Bausteine, die zur Erstellung von Speicherklassen kombiniert werden.

Gängige Richtlinientypen sind:

- **Leistungsrichtlinien** – Latenzziele, IOPS oder Anforderungen an den Durchsatz definieren.
- **Kapazitätsrichtlinien** – Bereitstellungsmodus, Schwellenwertwarnungen oder Wachstumsgrenzen festlegen.
- **Sicherheitsrichtlinien** – Anforderungen an Verschlüsselung, Compliance oder Zugriffskontrolle definieren.
- **Datenschutzrichtlinien** – Snapshot-Zeitpläne, Replikationsziele oder Aufbewahrungsfristen festlegen.

Richtlinien werden unabhängig voneinander definiert und anschließend beim Erstellen einer Speicherklasse kombiniert. So lässt sich dieselbe Leistungsrichtlinie für mehrere Klassen wiederverwenden oder eine Kapazitätsrichtlinie an einer zentralen Stelle aktualisieren und diese Änderung auf alle Klassen anwenden, die sie verwenden.

Was Speicherklassen sind

Eine Speicherklasse ist eine benannte Vorlage, die aus einer oder mehreren Richtlinien zusammengestellt wird. Sie erfasst die Speicherstandards Ihrer Organisation für einen bestimmten Workload-Typ.

Beispielsweise kann eine **Production Database** Speicherklasse erstellt werden, die hohe Leistung, hohe Verfügbarkeit und strenge Datenschutzrichtlinien kombiniert, oder eine **Development File Share** Speicherklasse, die moderate Leistung, flexible Kapazität und grundlegende Datenschutzrichtlinien kombiniert.

Speicheradministratoren definieren Speicherklassen, um Unternehmensanforderungen abzubilden. Alle Bereitstellungsaktivitäten, ob manuell, über geführte Workflows oder automatisiert, greifen auf die von diesen Administratoren genehmigte Bibliothek von Klassen zurück.

Wie Speicherklassen Standards durchsetzen

Bei der Speicherbereitstellung wird eine Speicherklasse ausgewählt, anstatt einzelne Einstellungen zu konfigurieren. Die lokale Bereitstellung über die NetApp Console nutzt die Richtlinien dieser Klasse, um zu ermitteln, welche Cluster in Ihrer Flotte über ausreichende Kapazität und Leistungsreserven zur Unterstützung der Arbeitslast verfügen, die optimale Platzierungsoption zu empfehlen und klassenbasierte Einstellungen automatisch bei der Bereitstellung anzuwenden.

Nach der Bereitstellung bewertet Console local deployment kontinuierlich jede Arbeitslast anhand der Standards ihrer Speicherklasse.

Speicherklassenabweichung und Konformität

Wenn eine Arbeitslast nicht mehr der vorgesehenen Speicherklasse entspricht, wird sie von der lokalen NetApp Console-Bereitstellung zur Untersuchung und Behebung markiert.

Die Probleme lassen sich in zwei Kategorien einteilen:

- **Konfigurationsabweichung**: Die durch die Speicherklassenrichtlinie festgelegten Speichereinstellungen entsprechen nicht mehr der beabsichtigten Konfiguration. Dies kann auftreten, wenn Änderungen direkt am ONTAP Cluster oder außerhalb standardmäßiger Bereitstellungsabläufe vorgenommen werden.
- **Nichteinhaltung der Leistungsanforderungen**: Das Laufzeitverhalten der Arbeitslast entspricht nicht mehr der Performance-Absicht der Speicherklasse (zum Beispiel kontinuierlicher Druck nahe einer QoS-Grenze oder erhöhte Tail-Latenz).

Eine Analyseansicht erläutert, was sich geändert hat und warum. Geführte Korrekturmaßnahmen (zum Beispiel **Fix it**) können zur Verfügung stehen, um die Compliance wiederherzustellen. Einige Korrekturen können direkt angewendet werden, während andere möglicherweise eine Zuordnung der Workload zu einer anderen Speicherklasse erfordern, um das beabsichtigte Verhalten wiederherzustellen.

Wo untersucht werden kann

Abweichungen und Nichteinhaltungen lassen sich in der Regel von einem dieser Orte aus untersuchen (die Verfügbarkeit hängt von Ihrer Bereitstellung und Ihren Berechtigungen ab):

- **Speicherklassen:** Drift / Compliance
- **Warnungen:** Analysieren

Schritt-für-Schritt-Anweisungen sind unter Speicherklassenabweichung beheben zu finden.

End-to-End-Workflow

Die folgenden Schritte beschreiben den Prozess zur Verwendung von Speicherklassen zur Standardisierung und Steuerung des Speichers in Ihrer Umgebung:

1. **Speicherklassenrichtlinien erstellen** – Richtlinien definieren die einzelnen Dimensionen des Speicherverhaltens (Leistungsziele, Kapazitätseinstellungen, Sicherheitsanforderungen, Datensicherungszeitpläne). Richtlinien werden erstellt, bevor eine Speicherklasse aufgebaut wird.
2. **Speicherklasse erstellen** – Eine Speicherklasse wird zusammengestellt, indem jeweils eine Richtlinie aus jeder zutreffenden Kategorie kombiniert wird. Es kann eine vordefinierte Speicherklasse verwendet oder eine benutzerdefinierte Speicherklasse für die Standards Ihrer Organisation erstellt werden.
3. **Die Speicherklasse mit einer Flotte verknüpfen** - Nach dem Erstellen einer Speicherklasse erfolgt die Verknüpfung mit der Flotte, in der sie für die Bereitstellung und die Compliance-Überwachung verwendet wird.
4. **Speicherbereitstellung mithilfe der Speicherklasse** – Beim Bereitstellen eines Volumes oder einer LUN wird eine Speicherklasse ausgewählt, anstatt einzelne Einstellungen zu konfigurieren. Die lokale Bereitstellung über die Konsole verwendet die Klasse, um die optimale Clusterplatzierung zu empfehlen, anschließend erfolgt die Bereitstellung mit den in der Klasse definierten Einstellungen.
5. **Überwachung von Workloads auf Abweichungen** – Die lokale NetApp Console-Bereitstellung bewertet kontinuierlich jeden Workload anhand der in seiner Speicherklasse kodierten Standards. Treten Konfigurationsabweichungen oder eine Nichteinhaltung der Leistungsanforderungen auf, wird das Problem gekennzeichnet und möglicherweise eine Warnung ausgelöst.
6. **Abweichungen beheben, um die Konformität wiederherzustellen** - Wenn Abweichungen oder Leistungsmängel festgestellt werden, besteht die Möglichkeit, geführte Schritte zur manuellen Behebung des Problems zu nutzen, die Console lokale Bereitstellung häufige Abweichungsbedingungen automatisch beheben zu lassen oder eine Arbeitslast von ihrer Speicherklasse zu trennen, falls eine Änderung der Einstellungen erforderlich ist.

Wie Speicherklassen mit Flotten funktionieren

Speicherklassen sind Flotten zugeordnet. Wenn eine Speicherklasse einer Flotte zugeordnet wird, steht diese Klasse für alle Bereitstellungen innerhalb der Flotte zur Verfügung. Dies stellt sicher, dass jede in der Flotte bereitgestellte Workload denselben Standards folgt, wodurch Flotten die primäre Methode sind, um ein konsistentes Speicherverhalten über verwandte Cluster hinweg durchzusetzen.

Weitere Informationen zur Organisation von Flotten finden Sie unter "Informationen zum Flottenmanagement in der lokalen NetApp Console-Bereitstellung".

Wie es weitergeht

- Informationen zur Organisation der Flotte finden Sie unter "Informationen zum Flottenmanagement in der lokalen NetApp Console-Bereitstellung".
- Informationen zum Erstellen von Richtlinien und Speicherklassen sind unter "Speicherklassen und Richtlinien verwalten" zu finden.
- "Speicher manuell bereitstellen"
- "Speicher automatisch bereitstellen"
- "Speicher mit KI-Unterstützung bereitstellen"
- Zur Analyse und Behebung von Drift siehe "Speicherklassenabweichung beheben"

Verständnis der Speicherklassenrichtlinien in der lokalen NetApp Console-Bereitstellung

Speicherklassenrichtlinien sind die Bausteine, aus denen eine Speicherklasse erstellt wird. Jede Richtlinie steuert einen bestimmten Aspekt des Speicherverhaltens. Wenn Richtlinien zu einer Speicherklasse kombiniert werden, entsteht eine wiederverwendbare Vorlage, die die NetApp Console lokale Bereitstellung automatisch zum Bereitstellungszeitpunkt durchsetzt und während des gesamten Lebenszyklus einer Arbeitslast kontinuierlich überwacht.

Richtlinien als Bausteine

Eine Speicherklasse besteht aus einer oder mehreren Richtlinien, die jeweils eine andere Dimension des Speicherverhaltens regeln. Speicheradministratoren definieren Richtlinien, um Unternehmensstandards wie Leistungserwartungen, Kapazitätsgrenzen und Datenplatzierungsregeln abzubilden, und stellen diese anschließend zu Speicherklassenvorlagen zusammen. Wenn eine Arbeitslast mithilfe einer Speicherklasse bereitgestellt wird, übernimmt sie alle Richtlinien dieser Klasse. Dieses Design trennt die Verantwortung für die Definition von Standards von der Bereitstellung, sodass Speicher konsistent durch automatisierte Workflows bereitgestellt werden kann, ohne dass individuelle Konfigurationsentscheidungen erforderlich sind.

Arten von Speicherklassenrichtlinien

NetApp Console lokale Bereitstellung umfasst vier Arten von Richtlinien, die zur Erstellung von Speicherklassen verwendet werden können:

Leistungsrichtlinie
: Eine Leistungsrichtlinie legt die erwarteten IOPS/TB, die maximalen IOPS/TB, die absoluten minimalen IOPS und die erwarteten Latenzziele für eine Arbeitslast fest. Die lokale Bereitstellung der Console verwendet diese Werte, um bei der Bereitstellung Cluster mit ausreichendem Leistungsspielraum zu empfehlen und Abweichungen bei IOPS oder Latenz nach der Bereitstellung zu erkennen.

Kapazitätsrichtlinie
: Eine Kapazitätsrichtlinie steuert, wie ein Volume Speicherplatz belegt und verwaltet. Sie legt die Speicherplatzreservierung (thick, thin oder Systemstandard), das automatische Wachstum, FabricPool Tiering sowie fest, ob NAS-Workloads als FlexVol oder FlexGroup Volumes bereitgestellt werden.

Sicherheitsrichtlinie
: Eine Sicherheitsrichtlinie legt die Anforderungen für Verschlüsselung, Ransomware-Schutz und FIPS für eine Arbeitslast fest. Jedes Attribut kann auf einen erforderlichen Wert gesetzt oder auf „beliebig“ belassen werden, um die Systemvorgabe zu übernehmen.

Datensicherungsstrategie
: Eine Datensicherungsstrategie legt die Anzahl der in jedem Intervall aufbewahrten Snapshots fest, damit Workloads, die die Strategie verwenden, einen konsistenten Sicherungsplan erhalten.

Standardrichtlinien

Die lokale Bereitstellung über die Console umfasst systemdefinierte Richtlinien für alle vier Richtlinientypen. Diese Richtlinien können beim Erstellen einer Speicherklasse unverändert verwendet oder als Ausgangspunkt für benutzerdefinierte Richtlinien kopiert werden, die auf die Anforderungen Ihrer Organisation zugeschnitten sind.

Leistungsrichtlinien

Name	Typ	Erwartete IOPS/TB	Maximale IOPS/TB	Absolute minimale IOPS	Erwartete Latenz (ms)	Zusammenfassung
Extrem für Datenbankdaten	System definiert	12.288	24.576	2.000	1	Verwendung für transaktionale Datenbank-Datenvolumen, die kontinuierlich hohe IOPS und Latenzzeiten im Submillisekundenbereich erfordern.
Extrem für Datenbankprotokolle	System definiert	22.528	45.056	4.000	1	Für Datenbanktransaktionsprotokoll-Volumes, die den höchsten IOPS-Mindestwert erfordern, um Schreibengpässe zu verhindern.
Extrem für gemeinsam genutzte Datenbankdaten	System definiert	16.384	32.768	2.000	1	Für gemeinsam genutzte Datenbank-Volumes, auf die mehrere Hosts zugreifen und die hohen Durchsatz sowie konstante Latenz erfordern.
Extreme Performance	System definiert	6.144	12.288	1.000	1	Verwendung für HPC-, KI/ML- und Analyse-Workloads, die hohe Burst-IOPS und vorhersehbar niedrige Latenz erfordern.
Performance	System definiert	2.048	4.096	500	2	Verwendung für virtualisierte und Unternehmensanwendungen, die eine zuverlässige Leistung ohne extreme IOPS-Anforderungen benötigen.
Wert	System definiert	128	512	75	17	Geeignet für kostensensitive Workloads wie Home-Verzeichnisse, Dateifreigaben und Archive.

Kapazitätsrichtlinien

Name	Typ	Speicherplatzreservierung	Autowachstumsmodus	Tiering-Richtlinie	Volume-Typ (NAS)	Zusammenfassung
Standard	System definiert	Systemstandard	Systemstandard	keine	Systemstandard	Für allgemeine Arbeitslasten geeignet, bei denen das standardmäßige Kapazitätsverhalten der Plattform akzeptabel ist.

Name	Typ	Speicherplatzreservierung	Autowachstumsmodus	Tiering-Richtlinie	Volume-Typ (NAS)	Zusammenfassung
Produktion	System definiert	Systemstandard	wachsen	keine	Systemstandard	Für Produktionsworkloads geeignet, die sich automatisch erweitern müssen, um Ausfälle aufgrund von Speicherplatzmangel zu verhindern.

Sicherheitsrichtlinien

Name	Typ	Verschlüsselung	Schutz vor Ransomware	FIPS	Zusammenfassung
Standard	System definiert	beliebig	beliebig	beliebig	Für Arbeitslasten geeignet, bei denen das standardmäßige Sicherheitsverhalten der Plattform akzeptabel ist.
Anti-Ransomware	System definiert	beliebig	am	beliebig	Zur Verwendung bei Arbeitslasten mit sensiblen oder geschäftskritischen Daten, die einen aktiven Ransomware-Schutz erfordern.
Produktion	System definiert	aktiviert	beliebig	beliebig	Zur Verwendung bei Produktionsworkloads, bei denen Verschlüsselung aus Compliance-Gründen erforderlich ist.

Datensicherungsstrategien

Name	Typ	Stündliche Momentaufnahmen	Tagesaufnahmen	Wöchentliche Momentaufnahmen	Monatliche Momentaufnahmen	Zusammenfassung
Standard	System definiert	6	2	2	0	Geeignet für Standard-Workloads, die kurzfristige Wiederherstellungspunkte ohne langfristigen Aufbewahrungsaufwand erfordern.

Name	Typ	Stündliche Momentaufnahmen	Tagesaufnahmen	Wöchentliche Momentaufnahmen	Monatliche Momentaufnahmen	Zusammenfassung
3-monatlich stündlich	System definiert	23	6	4	3	Zur Verwendung bei regulierten oder geschäftskritischen Arbeitslasten, die granulare Wiederherstellungspunkte innerhalb eines Tages und eine dreimonatige historische Aufbewahrung erfordern.

Vordefinierte Speicherklassenrichtlinien in der lokalen NetApp Console-Bereitstellung prüfen

NetApp Console lokale Bereitstellung umfasst systemdefinierte Richtlinien für alle vier Richtlinientypen. Diese Referenz dient dazu, diejenige Richtlinie zu identifizieren, die am besten zu den Anforderungen Ihres Workloads passt, wenn eine Speicherklasse erstellt oder angepasst wird.

Leistungsrichtlinien

Extreme Performance
: Verwendung für HPC-, KI/ML- und Analyse-Workloads, die hohe Burst-IOPS und vorhersehbar niedrige Latenz erfordern.

Extrem für Datenbankdaten
: Verwendung für transaktionale Datenbank-Datenvolumen, die kontinuierlich hohe IOPS und Latenzzeiten im Submillisekundenbereich erfordern.

Extrem für Datenbankprotokolle
: Für Datenbanktransaktionsprotokoll-Volumes, die den höchsten IOPS-Mindestwert erfordern, um Schreibengpässe zu verhindern.

Extrem für gemeinsam genutzte Datenbankdaten
: Für gemeinsam genutzte Datenbank-Volumes, auf die mehrere Hosts zugreifen und die hohen Durchsatz sowie konstante Latenz erfordern.

Performance
: Verwendung für virtualisierte und Unternehmensanwendungen, die eine zuverlässige Leistung ohne extreme IOPS-Anforderungen benötigen.

Wert
: Geeignet für kostensensitive Workloads wie Home-Verzeichnisse, Dateifreigaben und Archive.

Kapazitätsrichtlinien

Autogrow-Kapazität
: Für Produktionsworkloads geeignet, die sich automatisch erweitern müssen, um Ausfälle aufgrund von Speicherplatzmangel zu verhindern.

Sicherheitsrichtlinien

Verschlüsselung ruhender Daten

Zur Verwendung bei Produktionsworkloads, bei denen Verschlüsselung aus Compliance-Gründen erforderlich ist.

Schutz vor Ransomware

Zur Verwendung bei Arbeitslasten mit sensiblen oder geschäftskritischen Daten, die einen aktiven Ransomware-Schutz erfordern.

Standardsicherheit

Für Arbeitslasten geeignet, bei denen das standardmäßige Sicherheitsverhalten der Plattform akzeptabel ist.

Datensicherungsstrategien

Standard

Geeignet für Standard-Workloads, die kurzfristige Wiederherstellungspunkte ohne langfristigen Aufbewahrungsaufwand erfordern.

3-monatlich stündlich

Zur Verwendung bei regulierten oder geschäftskritischen Workloads, die granulare Wiederherstellungspunkte innerhalb eines Tages und eine dreimonatige historische Aufbewahrung erfordern.

30-tägige Wiederherstellung

Geeignet für Standard-Workloads, die kurzfristige Wiederherstellungspunkte ohne langfristigen Aufbewahrungsaufwand erfordern.

90-tägige Wiederherstellung

Zur Verwendung bei regulierten oder geschäftskritischen Workloads, die granulare Wiederherstellungspunkte innerhalb eines Tages und eine dreimonatige historische Aufbewahrung erfordern.

Speicherklassen in der lokalen NetApp Console-Bereitstellung erstellen

Erstellen Sie eine Speicherklasse in der lokalen NetApp Console-Bereitstellung, um die Bereitstellung und Verwaltung von Speicher in Ihren Flotten zu standardisieren. Eine Speicherklasse ist eine wiederverwendbare Vorlage, die Speicherklassenrichtlinien wie Leistungsziele, Kapazitätsverhalten, Sicherheitsanforderungen und Zeitpläne für den Datenschutz in einer einzigen benannten Definition bündelt.

Wenn Benutzer (oder eine Automatisierung) ein Volume oder eine LUN mithilfe einer Speicherklasse bereitstellen, wendet NetApp Console Local Deployment automatisch die Richtlinien der Klasse an. Nach der Bereitstellung überwacht Console Local Deployment kontinuierlich die Workloads in Bezug auf die Speicherklasse, um Abweichungen zu erkennen und kann Korrekturmaßnahmen zur Wiederherstellung der Compliance einleiten oder automatisieren.

Bevor Sie beginnen

- Mindestens ein ONTAP Cluster muss erkannt werden, damit die lokale Bereitstellung der Konsole Ziele für Platzierungsempfehlungen hat.

- Stellen Sie sicher, dass Sie über die Rolle des Organisationsadministrators verfügen (oder über eine Rolle, die in Ihrer Umgebung Berechtigungen zur Speicherklassenverwaltung gewährt).
- Erstellen (oder identifizieren) Sie die Speicherklassenrichtlinien, die Sie verwenden möchten, Leistung, Kapazität, Sicherheit und Datenschutz, da Speicherklassen aus Richtlinien zusammengesetzt werden.

Erstellen Sie eine Speicherklasse

Zum Hinzufügen einer Speicherklasse ist die Rolle „Organisationsadministrator“, „Ordneradministrator“ oder „Flottenadministrator“ erforderlich.

Schritte

1. **Speicher > Verwaltung** auswählen.
2. **Speicherklassen** auswählen.
3. Wählen Sie **Add**.
4. Unter **Grundlegende Informationen** Folgendes eingeben:
   - **Name der Storage-Klasse**: Einen eindeutigen Namen für die Storage-Klasse eingeben.
   - **Beschreibung**: (Optional) Eine Beschreibung der Speicherklasse kann eingegeben werden.
   - **Empfohlene Apps**: (Optional) Eine Liste empfohlener Apps für die Speicherklasse kann eingegeben werden.
5. Unter **Speicherrichtlinien** eine oder mehrere Richtlinien auswählen, die mit der Speicherklasse verknüpft werden.
6. Wählen Sie **Add**.

Eine bestehende Speicherklasse anpassen

Die Rolle „Organization admin“, „Folder admin“ oder „fleet admin“ ist erforderlich, um eine bestehende Speicherklasse anzupassen.

Schritte

1. **Speicher > Verwaltung** auswählen.
2. **Speicherklassen** auswählen.
3. Für die Speicherklasse, die angepasst werden soll, **…** auswählen und dann **Duplizieren** auswählen.
4. Unter **Grundlegende Informationen** können die folgenden Angaben nach Bedarf aktualisiert werden:
   - **Name der Storage-Klasse**: Einen eindeutigen Namen für die Storage-Klasse eingeben.
   - **Beschreibung**: (Optional) Eine Beschreibung der Speicherklasse kann eingegeben werden.
   - **Empfohlene Apps**: (Optional) Eine Liste empfohlener Apps für die Speicherklasse kann eingegeben werden.
5. Unter **Speicherrichtlinien** eine oder mehrere Richtlinien auswählen, die mit der Speicherklasse verknüpft werden.
6. Wählen Sie **Add**.

Bearbeiten einer benutzerdefinierten Speicherklasse

Zum Bearbeiten einer benutzerdefinierten Speicherklasse ist die Rolle „Organization admin“, „Folder admin“ oder „fleet admin“ erforderlich.

Schritte

1. **Speicher > Verwaltung** auswählen.
2. **Speicherklassen** auswählen.
3. Wählen Sie für die Speicherklasse, die Sie bearbeiten möchten, **…** und dann **Bearbeiten** aus.
4. Unter **Grundlegende Informationen** können die folgenden Angaben nach Bedarf bearbeitet werden:
   - **Name der Storage-Klasse**: Einen eindeutigen Namen für die Storage-Klasse eingeben.
   - **Beschreibung**: (Optional) Eine Beschreibung der Speicherklasse kann eingegeben werden.
   - **Empfohlene Apps**: (Optional) Eine Liste empfohlener Apps für die Speicherklasse kann eingegeben werden.
5. Unter **Speicherrichtlinien** eine oder mehrere Richtlinien auswählen, die mit der Speicherklasse verknüpft werden.
6. **Bearbeiten** auswählen.

Löschen einer benutzerdefinierten Speicherklasse

Zum Löschen einer benutzerdefinierten Speicherklasse ist die Rolle „Organization admin“, „Folder admin“ oder „fleet admin“ erforderlich.

Schritte

1. **Speicher > Verwaltung** auswählen.
2. **Speicherklassen** auswählen.
3. Für die Speicherklasse, die gelöscht werden soll, **…** auswählen und dann **Löschen** wählen.
4. Wählen Sie **Delete**.

   Beachten Sie, dass diese Aktion nicht rückgängig gemacht werden kann. Wenn eine Speicherklasse gelöscht wird, die aktuell verwendet wird, funktionieren alle mit dieser Klasse bereitgestellten Volumes oder LUNs weiterhin, sind aber nicht mehr der gelöschten Klasse zugeordnet.

Speicher in der lokalen NetApp Console-Bereitstellung bereitstellen

Volumes und LUNs in der lokalen NetApp Console-Bereitstellung bereitstellen, damit Speicherressourcen für Ihre Workloads verfügbar sind. Während der Bereitstellung kann optional eine Speicherklasse ausgewählt werden, um vordefinierte Speicherrichtlinien und Organisationsstandards anzuwenden.

Erforderliche Zugriffsrollen

Superadministrator, Organisationsadministrator, Ordner- oder Flottenadministrator oder Speicheradministrator. "Informationen zu Zugriffsrollen".

Ein Volume bereitstellen

Schritte

1. **Speicher > Verwaltung** auswählen.
2. **Flotten** auswählen.
3. Wählen Sie die Flotte aus, in die Sie bereitstellen möchten.

4. Wählen Sie **Add**.
5. Im Menü **Volume** auswählen.
6. Unter **Volumendetails**:
    a. Geben Sie einen Volume-Namen ein.
    b. Kapazität eingeben (und bei Bedarf die Einheiten auswählen).
    c. (Optional) Wählen Sie eine Speicherklasse aus, auf die Speicherklassenrichtlinien angewendet werden. Wenn keine ausgewählt wird, wird das Volume ohne Speicherklassenrichtlinien bereitgestellt.
7. Unter **Systemdetails**:
    a. Ein System aus den für die ausgewählte Flotte berechtigten Systemen auswählen.
    b. Eine Storage-VM auswählen.
8. Unter **Host (NAS)-Details** kann ausgewählt werden, wie Hosts auf das Volume zugreifen:
    a. Export per NFS (Exportrichtlinien steuern, welche NFS-Hosts auf das Volume zugreifen können)
    b. Freigabe über SMB/CIFS
9. Wählen Sie **Add**.

Eine LUN bereitstellen

Schritte

1. **Speicher > Verwaltung** auswählen.
2. **Flotten** auswählen.
3. Wählen Sie die Flotte aus, in die Sie bereitstellen möchten.
4. Wählen Sie **Add**.
5. Im Menü die Option **LUNs** auswählen.
6. Unter **LUN-Speicherdetails**:
    a. Geben Sie einen Präfixnamen ein.
    b. Geben Sie die Anzahl der LUNs ein, die mit diesem Präfix erstellt werden.
    c. Geben Sie die Kapazität pro LUN ein (und wählen Sie bei Bedarf die Einheiten aus).
    d. (Optional) Wählen Sie eine Speicherklasse aus, auf die Speicherklassenrichtlinien angewendet werden. Wenn keine ausgewählt wird, werden die LUNs ohne Speicherklassenrichtlinien bereitgestellt.
7. Unter **Systemdetails**:
    a. Wählen Sie ein System aus (falls dazu aufgefordert wird).
    b. Eine Storage-VM auswählen.
8. Unter **Host (SAN) Details** kann ausgewählt werden, wie Hosts auf das Volume zugreifen:
    a. Das Host-Betriebssystem (zum Beispiel Windows oder Linux) auswählen, um empfohlene Standardwerte für die LUN-Ausrichtung und die Blockgröße festzulegen.
    b. Die Host-Mapping-Gruppe steuert, welche Initiatoren auf die LUNs zugreifen können.
9. Wählen Sie **Add**.

Speicherzustand überwachen

Speicherüberwachung in der lokalen NetApp Console-Bereitstellung

NetApp Console lokale Bereitstellung unterstützt die Überwachung von Speicher über Flotten hinweg mit Dashboards, Warnmeldungen, detaillierten Analysen und Abhilfemaßnahmen, sodass Probleme erkannt und behoben werden können, bevor sie sich auf Workloads auswirken.

Die Flottenintegrität lässt sich mit Dashboards überwachen.

Beginnen Sie mit Dashboards für einen schnellen Überblick über Speicherzustand und Performance. Die Startseite bietet Kennzahlen auf einen Blick, die Dashboard-Tabelle enthält vordefinierte und benutzerdefinierte Dashboards, und bei Bedarf stehen Bereiche für Warnungen, Untersuchung und Behebung für detailliertere Informationen zur Verfügung.

- "Startseitenmetriken in der lokalen NetApp Console-Bereitstellung anzeigen"
- "Dashboards in der lokalen NetApp Console-Bereitstellung aktuell halten"
- "Informationen zu benutzerdefinierten Dashboards in der lokalen NetApp Console-Bereitstellung"

Leistungsprobleme untersuchen

Mit dem Workload Analyzer lassen sich Leistungsprobleme auf einzelnen Volumes untersuchen. Er korreliert Latenz, Durchsatz, IOPS und Konfigurationsänderungen, sodass die Ursachen genau identifiziert werden können.

- "Informationen zum NetApp Console lokalen Deployment Workload Analyzer"
- "Hohe Latenz auf einem Volume in der lokalen NetApp Console-Bereitstellung untersuchen"
- "Untersuchung eines hohen Durchsatzbedarfs auf einem Volume in der lokalen NetApp Console-Bereitstellung"
- "Informationen zu den Metriken des Workload Analyzers in der lokalen NetApp Console-Bereitstellung"

Warnungen und Benachrichtigungen konfigurieren

Warnrichtlinien und Benachrichtigungskanäle werden so konfiguriert, dass die richtigen Personen über Speicherzustände informiert werden, die Aufmerksamkeit erfordern. Beispielsweise kann eine Kapazitätswarnung an das Speicherteam und eine Schutzwarnung an den Backup-Administrator weitergeleitet werden, der darauf reagieren kann.

"Benachrichtigungen und Alarmrichtlinien in der lokalen Bereitstellung der NetApp Console konfigurieren". "Speicherwarnungen in der lokalen NetApp Console-Bereitstellung anzeigen".

Probleme beheben

Wenn ein Problem erkannt wird, kann es direkt aus der lokalen NetApp Console-Bereitstellung behoben werden:

- **Automatisierte Fehlerbehebung** – Die lokale NetApp Console-Bereitstellung wendet Korrekturmaßnahmen automatisch auf Basis vordefinierter Regeln an.
- **Geführte Problembehebung** – Schrittweise Empfehlungen stehen zur Verfügung, um Probleme mit voller

Kontrolle über jede Aktion zu beheben.

Überwachung mit Dashboards

Startseitenmetriken in der lokalen NetApp Console-Bereitstellung anzeigen

Das Dashboard der Startseite in der lokalen NetApp Console-Bereitstellung dient als Standard-Ausgangspunkt für die Überwachung von Speicherzustand und -leistung. Es bietet wichtige Kennzahlen zu Flottenzustand, Warnmeldungen, Sicherheit, Kapazitätsauslastung, Latenz, Durchsatz und IOPS.

Das Dashboard auf der Startseite ist automatisch auf nur die Flotten und Systeme beschränkt, die Sie anzeigen dürfen. Außerdem kann der Startseite ein benutzerdefiniertes Dashboard für die rollenspezifische Überwachung hinzugefügt werden.

Die Karten dienen als mehrstufiger Triage-Workflow. Zunächst bieten **Fleet health** und **Alerts** einen Überblick über Risikobereiche. **System health status** und **Recommended remediations** ermöglichen die Identifizierung betroffener Ressourcen. **Capacity usage**, **Latency**, **Throughput** und **IOPS** unterstützen die Untersuchung der Ursachen.

Flottengesundheit

Die Karte **Fleet health** zeigt eine Übersicht auf hoher Ebene für die fünf wichtigsten Flotten, einschließlich Systemanzahl, genutzter Kapazität, Sicherheitskonformität und kritischer Warnmeldungen. Mit dieser Karte lässt sich feststellen, welche Flotten sofortige Aufmerksamkeit erfordern. Durch Auswahl des Flottennamens wird ein ausschließlich für diese Flotte bestimmtes Dashboard angezeigt.

Empfohlene Abhilfemaßnahmen

Die Karte „Empfohlene Abhilfemaßnahmen“ listet aktive Probleme und empfohlene Maßnahmen auf. Die Karte priorisiert Abhilfemaßnahmen basierend auf Kapazitätsdruck, Offline-Ressourcen und schutzbezogenen Risiken.

Warnmeldungen

Die **Warnungen**-Karte fasst das Warnaufkommen im ausgewählten Zeitraum zusammen und gruppiert es nach Schweregrad. Mit dieser Karte lässt sich die aktuelle Anzahl an Vorfällen nachvollziehen und es werden kürzliche Änderungen bei kritischen, Warn- oder Informationswarnungen sichtbar.

Sicherheit

Die **Security**-Karte fasst Compliance- und Schutzkennzahlen zusammen, wie Systemkonformität und ransomware-bezogene Kontrollen. In dieser Ansicht lassen sich Sicherheitstrends über Ihre Ressourcen hinweg überwachen.

Kapazitätsauslastung

Die Karte **Kapazitätsauslastung** zeigt prognostizierte und historische Nutzungstrends ausgewählter Flotten oder Systeme an. Mit dieser Karte lassen sich Wachstumsmuster erkennen und zusätzliche Kapazitäten planen.

Latenz

Die **Latenz**-Karte erfasst das Reaktionszeitverhalten im Zeitverlauf über die ausgewählten Systeme hinweg.

Dieser Trend ermöglicht das Erkennen aufkommender Leistungsverzögerungen und den Vergleich der relativen Latenz zwischen Ressourcen.

Durchsatz

Die **Durchsatzkarte** zeigt Datentransferraten im Zeitverlauf für ausgewählte Systeme an. Mit dieser Karte lassen sich die Auslastungsintensität nachvollziehen und Änderungen der Durchsatzanforderungen überwachen.

IOPS

Die **IOPS**-Karte zeigt die Ein-/Ausgabe-Betriebsraten im Zeitverlauf an. Mit dieser Karte lassen sich die Aktivitätsniveaus zwischen Systemen vergleichen und kontinuierlicher oder intermittierender E/A-Bedarf erkennen.

Dashboard-Karte (Beispiel für eine Metrikkarte)

Der untere Bereich **Dashboard** kann ein vom Benutzer ausgewähltes benutzerdefiniertes Dashboard enthalten, beispielsweise die durchschnittliche Latenz für einen ausgewählten Produktionsbereich. Diese Karten ermöglichen ein fokussiertes Monitoring nach Team, Workload oder Ziel.

Systemgesundheitsstatus

Die Karte **System health status** listet die einzelnen Systeme mit ihrem aktuellen Zustand auf. Mit dieser Karte lassen sich fehlerhafte Systeme schnell identifizieren und Statusänderungen mit Warnmeldungen und Leistungssignalen in Zusammenhang bringen.

Verwandte Informationen

- "Informationen zu benutzerdefinierten Dashboards in der lokalen NetApp Console-Bereitstellung"
- "Informationen zu benutzerdefinierten Dashboard-Karten und Metriken in der lokalen NetApp Console-Bereitstellung"

Benutzerdefinierte Dashboards verwenden

Informationen zu benutzerdefinierten Dashboards in der lokalen NetApp Console-Bereitstellung

Benutzerdefinierte Dashboards in der lokalen NetApp Console-Bereitstellung ermöglichen die Erstellung fokussierter Überwachungsansichten für bestimmte Teams, Flotten, Workloads und operative Ziele. Benutzerdefinierte Dashboards ergänzen das Dashboard der Startseite, indem sie gezielte Sichtbarkeit zur umfassenden, stets verfügbaren Überwachung hinzufügen.

Wie Dashboard-Typen zusammenarbeiten

Startseite Dashboard
: Sofort einsatzbereite Überwachungsbereiche für Kapazität, Warnmeldungen, Leistungskapazität, Lizenzen und Datenschutzstatus. Die Ansichten sind vorkonfiguriert und werden automatisch aktualisiert. "Startseitenmetriken in der lokalen NetApp Console-Bereitstellung anzeigen".

Benutzerdefinierte Dashboards
: Rollenspezifische Überwachungsansichten, die aus vordefinierten Karten erstellt sind, einschließlich auswählbarem Bereich, Metriken, Zielressourcen und Zeitfenstern.

Beides zusammen verwenden: * Auf der Startseite mit der täglichen Basisüberwachung beginnen. * Benutzerdefinierte Dashboards für gezielte Untersuchungen nach Team, Flotte, Arbeitslast oder betrieblicher Fragestellung nutzen.

Sie können jeweils nur ein benutzerdefiniertes Dashboard zur Startseite hinzufügen.

Informationen zu benutzerdefinierten Dashboards

Ein benutzerdefiniertes Dashboard ist eine gespeicherte Sammlung von Karten, die Sie in einem Raster anordnen. Jede Karte basiert auf einer vordefinierten Kartenvorlage mit einer Kennzahl und einem Diagrammtyp. Wenn eine Karte hinzugefügt wird, werden Geltungsbereich, Zielobjekte, Aggregation und Zeitfenster konfiguriert.

Benutzerdefinierte Dashboards und Karten sind privat für Sie. Jede Karte zeigt nur Daten der Speicherressourcen an, zu deren Anzeige Sie berechtigt sind.

Sie können das benutzerdefinierte Dashboard von Ihrer Startseite entfernen und ein anderes hinzufügen, wenn sich die Überwachungsprioritäten ändern.

Überwachen Sie, was wichtig ist

Kartenvorlagen sind nach Metriktyp organisiert, sodass ein Dashboard auf einen bestimmten Betriebsbereich fokussiert werden kann. Beispielsweise können Kapazitätskarten genutzt werden, um ein Volumen zu überwachen, das schneller als erwartet wächst, oder Alarmkarten, um wiederholte Ausfälle in einem stark ausgelasteten Cluster zu verfolgen:

Performance
: Latenz, IOPS, Durchsatz, Auslastung und Leistungskapazität über die gesamte Flotte, Systeme, SVMs, Volumes und LUNs hinweg.

Kapazität
: Verwendete Kapazität, freie Kapazität, prozentual genutzte Kapazität und Snapshot-Kapazität über die gesamte Flotte, Systeme, SVMs, Volumes, LUNs und lokale Tiers.

Systemzustand
: Gesundheitszustand, Anzahl degradierter oder kritischer Objekte, ausgefallene Festplatten, Netzwerkschnittstellenfehler und Hot-Objekte.

Warnmeldungen
: Anzahl kritischer Warnmeldungen, Warnmeldungen nach Schweregrad, Warnmeldungen nach Wirkungsbereich, aktuelle Warnmeldungen und Warntrends im Zeitverlauf.

Einen vollständigen Katalog der vordefinierten Karten und Metriken enthält "Informationen zu benutzerdefinierten Dashboard-Karten und Metriken in der lokalen NetApp Console-Bereitstellung".

Ressourcentypen

Sie können Karten auf jeder Ebene der ONTAP Speicherhierarchie zuordnen: Flotte, Cluster, System (Knoten), SVM, Volume, LUN und lokale Ebene (Aggregat). Die verfügbaren Ressourcentypen hängen von der ausgewählten Kartenvorlage ab.

Plan Dashboard-Ansichten

Benutzerdefinierte Dashboards lassen sich um Ziele der Speicherverwaltung wie Workload-Performance-Triage, Kapazitätsplanung, Risikoerkennung und Priorisierung von Warnmeldungen organisieren.

Verwandte Informationen

- "Erste Schritte mit Dashboards in NetApp Console lokale Bereitstellung"
- "Startseitenmetriken in der lokalen NetApp Console-Bereitstellung anzeigen"
- "Informationen zu benutzerdefinierten Dashboard-Karten und Metriken in der lokalen NetApp Console-Bereitstellung"

Erste Schritte mit Dashboards in NetApp Console lokale Bereitstellung

In der lokalen NetApp Console-Bereitstellung umfasst der Workflow zur Überwachung von allgemeinen zu fokussierten Ansichten: Überprüfung des Dashboards auf der Startseite, Überprüfung vordefinierter Dashboards, Erstellung benutzerdefinierter Dashboards und Aktualisierung der Dashboards.

Erforderliche Zugriffsrollen

Alle Rollen. Dashboards zeigen nur die Ressourcen an, zu deren Anzeige Sie berechtigt sind. Wenn eine Ressource nicht in der Liste der verfügbaren Ressourcen erscheint, besteht keine Berechtigung zur Anzeige.

Ausgangszustand auf der Startseite prüfen

Das Dashboard auf der Startseite bietet einen Überblick über die Kapazität, Warnmeldungen, Leistung und den Status des Datenschutzes auf Organisationsebene.

- "Startseitenmetriken in der lokalen NetApp Console-Bereitstellung anzeigen"
- "Informationen zur Speicherüberwachung in der lokalen NetApp Console-Bereitstellung"

Weitere vordefinierte Dashboards anzeigen

Speicher > Dashboards öffnen, um vordefinierte Dashboards für zusätzliche, rollenbezogene Ansichten anzuzeigen.

- "Dashboards in der lokalen NetApp Console-Bereitstellung verwalten"

Benutzerdefinierte Dashboards für gezieltes Monitoring erstellen

Benutzerdefinierte Dashboards bieten gezielte Ansichten für ausgewählte Ressourcen, Kennzahlen und Zeitfenster.

- "Ein benutzerdefiniertes Dashboard erstellen"
- "Anpassen von Dashboard-Karten in der lokalen NetApp Console-Bereitstellung"

Dashboards aktuell halten

Dashboards können aktualisiert werden, wenn sich Prioritäten ändern, indem benutzerdefinierte Dashboards bearbeitet, dupliziert oder gelöscht werden.

- "Dashboards in der lokalen NetApp Console-Bereitstellung verwalten"
- "Informationen zu benutzerdefinierten Dashboard-Karten und Metriken in der lokalen NetApp Console-Bereitstellung"

Verwandte Informationen

- "Informationen zu benutzerdefinierten Dashboards in der lokalen NetApp Console-Bereitstellung"
- "Startseitenmetriken in der lokalen NetApp Console-Bereitstellung anzeigen"

Dashboards zur Überwachung von Zielen in der lokalen NetApp Console-Bereitstellung erstellen

Ein benutzerdefiniertes Dashboard in der lokalen NetApp Console-Bereitstellung erstellen, Karten hinzufügen und eine Überwachungsansicht für den täglichen Betrieb speichern.

Wenn lediglich eine sofort einsatzbereite Überwachung auf Organisationsebene benötigt wird, bieten sich vordefinierte Home-Page-Dashboards als Ausgangspunkt an. Ein benutzerdefiniertes Dashboard eignet sich, wenn eine rollenspezifische Ansicht, eine gezielte Ausrichtung auf Ressourcen oder ein individuell angepasstes Kartenlayout erforderlich ist.

Richtlinien für das Dashboard zur lokalen Konsolenbereitstellung

- Nur der Benutzer, der das Dashboard erstellt, kann es anzeigen. Dashboards können nicht mit anderen Benutzern geteilt werden, selbst wenn sie zur Console-Startseite hinzugefügt werden.
- Sie können nur Ressourcen anzeigen, für die Sie die Berechtigung haben. Wenn eine Ressource nicht in der Liste der verfügbaren Ressourcen angezeigt wird, haben Sie keine Berechtigung, sie anzuzeigen.
- Bevor Sie beginnen, die Metriktypen und Ressourcen identifizieren, die das Dashboard erfassen soll."Informationen zu benutzerdefinierten Dashboard-Karten und Metriken in der lokalen NetApp Console-Bereitstellung"

Ein Dashboard für Ihre Überwachungsziele erstellen

Ein Dashboard bietet einen zentralen Ort, um die für Ihre Rolle relevanten Kennzahlen wie Flottenzustand, Leistungsschwerpunkte und Alarmtrends zu überwachen.

Schritte

1. **Speicher > Dashboards** auswählen.
2. **Dashboard hinzufügen** auswählen.

   Die lokale Bereitstellung über die Konsole erstellt ein neues Dashboard mit einem Standardnamen und ohne Beschreibung.

3. **Karte hinzufügen** auswählen.
4. Den **Ressourcentyp** für die Karte auswählen, zum Beispiel Flotte, System oder Volumen, und anschließend Ressourcen aus der Liste der verfügbaren Ressourcen auswählen.
5. **Weiter** auswählen, um mit der Auswahl einer Kennzahl und eines Kartentyps fortzufahren.
6. Wählen Sie eine anzuzeigende Metrik aus. Die verfügbaren Metriken können nach Typ gefiltert werden: der **Metriktyp**: **Leistung**, **Kapazität**, **Status** oder **Warnungen**, oder es kann nach einer bestimmten Metrik anhand ihres Namens gesucht werden. Die verfügbaren Metriken hängen vom ausgewählten

Ressourcentyp ab.

"Informationen zu den verfügbaren Kennzahlen."

7. Eine Karte für die Aufnahme in das Dashboard auswählen und **Weiter** wählen.

   Sie können jeweils nur eine Karte auswählen. Die Kartenvorschau zeigt Live-Daten für die ausgewählte Metrik und den Ressourcentyp an.

8. Benennen Sie Ihre Karte. Der Name muss innerhalb des Dashboards eindeutig sein.
9. Die Kartenvorschau kann überprüft, ein Kartenname und eine Beschreibung eingegeben und anschließend **Hinzufügen** ausgewählt werden.
10. Diese Schritte für zusätzliche Karten wiederholen.
11. Das Stiftsymbol ermöglicht das Bearbeiten des Dashboard-Namens und der Beschreibung, um den Zweck zu erläutern.
12. Im Aktionsmenü rechts neben der Schaltfläche „Karte hinzufügen“ die Option **Dashboard speichern** auswählen.

    Das gespeicherte Dashboard ist unter **Speicher > Dashboards** verfügbar.

13. Optional kann dieses Dashboard zur Startseite hinzugefügt werden, indem im Aktionsmenü **Zur Startseite hinzufügen** ausgewählt wird. Das Dashboard wird zur Startseite hinzugefügt. Nur Sie können die von Ihnen erstellten benutzerdefinierten Dashboards anzeigen. Es wird nicht mit anderen geteilt.

Verwandte Informationen

- "Startseitenmetriken in der lokalen NetApp Console-Bereitstellung anzeigen"
- "Informationen zu benutzerdefinierten Dashboards in der lokalen NetApp Console-Bereitstellung"
- "Anpassen von Dashboard-Karten in der lokalen NetApp Console-Bereitstellung"
- "Dashboards in der lokalen NetApp Console-Bereitstellung verwalten"

Karten in der lokalen NetApp Console-Bereitstellung anpassen

In der lokalen NetApp Console-Bereitstellung lassen sich Dashboard-Karten anpassen, wenn der Fokus der Bediener auf die wichtigsten Signale gelegt werden soll, wie etwa SLA-Risiko, Kapazitätsdruck oder wiederkehrender Alarmrauschen. Dieses Thema dient dazu, Dashboard-Ansichten auf die operativen Entscheidungen auszurichten, die Ihr Team treffen muss.

Bevor Sie beginnen

- Ein Dashboard erstellen oder öffnen, auf dem Karten platziert werden sollen.
- Verfügbare Vorlagen und Kennzahlen in "Informationen zu benutzerdefinierten Dashboard-Karten und Metriken in der lokalen NetApp Console-Bereitstellung" einsehen.

Karten können hinzugefügt werden, während ein bestehendes Dashboard verfeinert wird.

Diese Option eignet sich, wenn ein bestehendes Dashboard verfeinert wird und schnell Karten hinzugefügt werden sollen, die eine bestimmte operative Frage beantworten.

Schritte

1. Öffnen Sie das Dashboard, dem Sie eine Karte hinzufügen möchten.
2. **Karte hinzufügen** auswählen.
3. Den **Ressourcentyp** für die Karte auswählen, zum Beispiel Flotte, System oder Volumen, und anschließend Ressourcen aus der Liste der verfügbaren Ressourcen auswählen.
4. **Weiter** auswählen, um mit der Auswahl einer Kennzahl und eines Kartentyps fortzufahren.
5. Wählen Sie eine anzuzeigende Metrik aus. Die verfügbaren Metriken können nach Typ gefiltert werden: der **Metriktyp**: **Leistung**, **Kapazität**, **Status** oder **Warnungen**, oder es kann nach einer bestimmten Metrik anhand ihres Namens gesucht werden. Die verfügbaren Metriken hängen vom ausgewählten Ressourcentyp ab.

   "Informationen zu den verfügbaren Kennzahlen."

6. Eine Karte für die Aufnahme in das Dashboard auswählen und **Weiter** wählen.

   Sie können jeweils nur eine Karte auswählen. Die Kartenvorschau zeigt Live-Daten für die ausgewählte Metrik und den Ressourcentyp an.

7. Benennen Sie Ihre Karte. Der Name muss innerhalb des Dashboards eindeutig sein.
8. Die Kartenvorschau kann überprüft, ein Kartenname und eine Beschreibung eingegeben und anschließend **Hinzufügen** ausgewählt werden.
9. Diese Schritte für zusätzliche Karten wiederholen.
10. Das Dashboard speichern.

Verwandte Informationen

- "Startseitenmetriken in der lokalen NetApp Console-Bereitstellung anzeigen"
- "Informationen zu benutzerdefinierten Dashboards in der lokalen NetApp Console-Bereitstellung"
- "Ein benutzerdefiniertes Dashboard erstellen"
- "Benutzerdefinierte Dashboards verwalten"
- "Informationen zu benutzerdefinierten Dashboard-Karten und Metriken in der lokalen NetApp Console-Bereitstellung"

Referenz auf vordefinierte Dashboards und benutzerdefinierte Dashboard Karten in der lokalen NetApp Console Bereitstellung

In der lokalen NetApp Console-Bereitstellung bieten vordefinierte Dashboards und benutzerdefinierte Dashboard-Kartenvorlagen eine Überwachung von ONTAP Leistung, Kapazität, Zustand und Alarmvorgängen.

Vordefinierte Dashboards

Folgende vordefinierte Dashboards sind sofort verfügbar.

Name	Beschreibung
Volumes	Volumenleistung, Kapazität, QoS, FabricPool, Wachstumsrate und Prognosemetriken.

Name	Beschreibung
Zeit bis zur vollständigen Auslastung	ONTAP Vorhersagen zur Laufzeit bis zur vollständigen Auslastung für Cluster, Volumes und Aggregate.
Sicherheit	Überblick über Sicherheitskonformität, Verschlüsselung, autonomen Ransomware-Schutz und Authentifizierung.
SVMs	ONTAP SVM Performance, Kapazität, Volume, LIF, Protokoll (CIFS, FCP, iSCSI, NFS, NVMe/FC), QoS und Latenz-Heatmap-Überwachung.
Leistung	Überwachung von Stromverbrauch, Temperatur und Lüfterdrehzahl für Knoten, Shelfs und Aggregate im ONTAP Cluster.
Nodes	ONTAP Knotenleistung, CPU, Netzwerk und Backend-Überwachung.
Netzwerk	Netzwerkleistungskennzahlen einschließlich Ethernet, FibreChannel, NVMe/FC, Link Aggregation Groups und Routen.
LUNs	Überwachung der ONTAP LUN-Leistung, Kapazität und Effizienz.
Systemzustand	ONTAP Clusterzustandsüberwachung einschließlich Fehlern, Warnungen, EMS-Alarme, HA-Problemen, Zustand von Knoten/Festplatten/Gehäusen, Volumes, Lizenzen und Netzwerkports.
Aggregate	ONTAP Gesamtkapazität, Effizienzkennzahlen und Wachstumsratenüberwachung.

Zeitfenster und Aggregation auf Dashboard-Ebene

Verfügbare Zeitfenster sind 30 Minuten, 1 Stunde, 24 Stunden, 48 Stunden, 7 Tage und 30 Tage. Die Aggregationsoptionen variieren je nach Vorlage und umfassen Ansichten wie Flottenweite-Rollup oder Top-N-Stil-Ergebnisse. Zeitfenster und Aggregation werden auf Dashboard-Ebene konfiguriert und gelten für alle Karten im Dashboard.

Dashboard-Kartenvorlagen und Metriken

Karten sind die Bausteine benutzerdefinierter Dashboards. Jede Karte verwendet eine vordefinierte Vorlage mit einer Metrik und einem Diagrammtyp und ordnet diese Ansicht dann bestimmten ONTAP Objekten und Überwachungszielen zu.

Kartenvorlagen sind vordefiniert und nicht benutzerdefiniert.

Index der Kennzahlen für Speicheroperationen (auf einen Blick)

Die Metriktypen orientieren sich an gängigen Ergebnissen der Speicherverwaltung, einschließlich Leistungsengpässen, Kapazitätsdruck, Gesundheitsrisiken und Alarmaufkommen.

Metrischer Typ	Unterstützte Metriken	Anwendungsfall für Storage-Administratoren	Detaillierte Vorlagen
Performance	Durchschnittliche Latenz, Spitzenlatenz, IOPS, Durchsatz (MB/s), Auslastung, Performance-Kapazität	Engpässe, kontinuierlichen Druck und Leistungsspielraum erkennen	Zu den Vorlagen

Metrischer Typ	Unterstützte Metriken	Anwendungsfall für Storage-Administratoren	Detaillierte Vorlagen
Kapazität	Belegte Kapazität, freie Kapazität, genutzte Kapazität (%), genutzte Snapshot-Kapazität	Wachstum nachverfolgen, Bereiche mit geringer freier Kapazität identifizieren und Snapshot-Auswirkungen überwachen	Zu den Vorlagen
Systemzustand	Gesundheitszustand, beeinträchtigte/kritische Objekte, ausgefallene Festplatten, Netzwerkschnittstellenfehler, Hot Objects (nach Latenz)	Gesundheitsrückschritte erkennen und operative Triage priorisieren	Zu den Vorlagen
Warnmeldungen	Warnungen (kritisch), Warnungen nach Schweregrad, Warnungen nach Wirkungsbereich, aktuelle Warnungen, Warnungstrend	Aktive Vorfälle und die Entwicklung des Alarmaufkommens im Zeitverlauf überwachen	Zu den Vorlagen

Unterstützte ONTAP Objekthierarchie (Ressourcentypen)

Kartendaten können auf mehreren ONTAP Objektebenen dargestellt werden, von der Flottenübersicht bis zur Fehlerbehebung auf Objektebene.

Ressourcentyp-Einstellungen entsprechen einer oder mehreren der folgenden Ressourcenebenen:

- Flotte
- Cluster
- System (Knoten)
- SVM
- Volumen
- LUN
- Lokale Ebene (Aggregate)

Die verfügbaren Ressourcenebenen hängen von der gewählten Vorlage und Metrik ab.

Diagrammtypen für die operative Analyse

Der Diagrammtyp beeinflusst, wie schnell Sie Trends, Vergleiche, Verteilungen und zeitpunktgenaue Werte interpretieren können.

Diagrammtyp	Am besten geeignet für
Liniendiagramm	Zeitreihen-Trends, wie Latenz, IOPS, Durchsatz, Auslastung und Alarmtrends im Zeitverlauf.
Balkendiagramm	Kategorischer Vergleich und Verteilung, z. B. Warnungen nach Schweregrad oder Impact-Bereich.
Kreisdiagramm oder Donut	Proportionale Verteilung, wie zum Beispiel der Prozentsatz der genutzten Kapazität.

Diagrammtyp	Am besten geeignet für
Tabelle	Detaillierte, mehrspaltige Daten, wie verwendete Kapazität, Gesundheitszustand und aktuelle Warnmeldungen.
Einzelne Zahl (stat)	Ein einzelner Schlüsselwert auf einen Blick, wie die Anzahl kritischer Warnmeldungen oder ausgefallener Festplatten.

Leistungsvorlagen für die Arbeitslast-Triage

Leistungsvorlagen konzentrieren sich auf Latenz-, Durchsatz- und Auslastungssignale, die auf Arbeitslastdruck hinweisen.

Vorlage	Diagrammtyp	Beschreibung
Durchschnittliche Latenz	Linie	Durchschnittliche Latenz der ausgewählten Ziele im gewählten Zeitfenster.
Spitzenlatenz	Linie	Maximale Latenz, die bei den ausgewählten Zielen im gewählten Zeitfenster beobachtet wurde.
IOPS	Linie	Summe der I/O-Operationen pro Sekunde über die ausgewählten Ziele hinweg.
Durchsatz (MB/s)	Linie	Summe des Datendurchsatzes über die ausgewählten Ziele.
Verwendung	Linie	Durchschnittliche CPU- oder Festplattenauslastung über die ausgewählten Ziele hinweg.
Performance-Kapazität	Tabelle	Headroom Analyse im Vergleich der aktuellen Auslastung zum optimalen Punkt.

Kapazitätsvorlagen für Wachstum und Spielraum

Kapazitätsvorlagen konzentrieren sich auf verbrauchten und verfügbaren Platz, um die Wachstumsplanung und Risikoerkennung zu unterstützen.

Vorlage	Diagrammtyp	Beschreibung
Verwendete Kapazität	Tabelle	Summe der genutzten Kapazität über die ausgewählten Ziele hinweg.
Freie Kapazität	Tabelle	Summe der freien oder verfügbaren Kapazität über die ausgewählten Ziele hinweg.
Verwendete Kapazität (%)	Kreisdiagramm oder Donut	Durchschnittliches Verhältnis von Verbrauch zu Gesamtmenge über die ausgewählten Ziele hinweg.
Verwendete Snapshot-Kapazität	Tabelle	Summe des von den ausgewählten Zielen belegten Snapshot-Speicherplatzes.

Gesundheitsvorlagen zur Risikoerkennung

Gesundheitsvorlagen konzentrieren sich auf Objektstatus und Fehlerindikatoren, um die operative Triage zu unterstützen.

Vorlage	Diagrammtyp	Beschreibung
Gesundheitszustand	Tabelle	Aktueller Gesundheitszustand für jedes ausgewählte Zielobjekt.
Beeinträchtigte/kritische Objekte	Einzelne Nummer	Anzahl der Objekte, deren Gesundheitszustand nicht OK ist.
Ausgefallene Festplatten	Einzelne Nummer	Summe der ausgefallenen Festplatten in den ausgewählten Systemen.
Netzwerkschnittstellenfehler	Kreisdiagramm oder Donut	Summe der Fehlerzähler der Netzwerkschnittstellen über die ausgewählten Ziele hinweg.
Hot Objects (nach Latenz)	Tabelle	Ressourcen, sortiert nach Spitzenlatenz, in absteigender Reihenfolge.

Alarmvorlagen zur Priorisierung von Vorfällen

Die Vorlagen für Warnmeldungen konzentrieren sich auf das Vorfallvolumen, den Schweregrad und den Auswirkungsbereich, um die Überwachung und Priorisierung zu unterstützen.

Vorlage	Diagrammtyp	Beschreibung
Warnungen (Kritisch)	Einzelne Nummer	Anzahl der Warnmeldungen mit kritischem Schweregrad innerhalb des Zeitfensters.
Warnungen nach Schweregrad	Bar	Warnmeldungen nach Schweregrad gruppiert.
Warnungen nach Wirkungsbereich	Bar	Warnmeldungen gruppiert nach Wirkungsbereich, wie Kapazität, Performance oder Sicherheit.
Aktuelle Warnmeldungen	Tabelle	Die aktuellsten Warnmeldungen, sortiert nach Zeit in absteigender Reihenfolge.
Alarmtrend	Linie	Anzahl der Alarme pro Zeitintervall im gewählten Zeitfenster.

Verwandte Informationen

- "Startseitenmetriken in der lokalen NetApp Console-Bereitstellung anzeigen"
- "Informationen zu benutzerdefinierten Dashboards in der lokalen NetApp Console-Bereitstellung"
- "Ein benutzerdefiniertes Dashboard erstellen"
- "Anpassen von Dashboard-Karten in der lokalen NetApp Console-Bereitstellung"
- "Benutzerdefinierte Dashboards verwalten"

Benutzerdefinierte Dashboards verwalten

Dashboards in der lokalen NetApp Console-Bereitstellung verwalten

Benutzerdefinierte Dashboards in der lokalen NetApp Console-Bereitstellung verwalten, um die Ansichten mit den Betriebsabläufen abzustimmen. Dashboards können bearbeitet, dupliziert und gelöscht werden, wenn sich Teams, Flotten und Prioritäten ändern.

Diese Aufgabe gilt nur für benutzerdefinierte Dashboards unter **Speicher > Dashboards**. Vordefinierte Startseiten Dashboards können nicht auf dieselbe Weise bearbeitet werden.

Dashboards anzeigen

Benutzerdefinierte und vordefinierte Dashboards anzeigen, um das gewünschte Dashboard zum Öffnen, Bearbeiten, Duplizieren oder Löschen zu finden.

Sie können ein vordefiniertes Dashboard duplizieren, um eine benutzerdefinierte Version zu erstellen, die Sie bearbeiten können.

Schritte

1. **Speicher > Dashboards** auswählen.
2. In der Dashboard-Tabelle kann das gewünschte Dashboard gefunden werden.
3. Den Namen des Dashboards auswählen, um es zu öffnen und die zugehörigen Kennzahlen anzuzeigen.
4. Bei Bedarf stehen verfügbare Aktionen zur Bearbeitung, Duplizierung oder Löschung benutzerdefinierter Dashboards zur Verfügung.

Ein Dashboard wird aktualisiert, wenn sich Prioritäten ändern

Ein Dashboard kann bearbeitet werden, wenn sich die betrieblichen Prioritäten ändern und eine Anpassung erforderlich ist, welche Karten und Kennzahlen sichtbar sind.

Schritte

1. **Speicher > Dashboards** auswählen.
2. Das zu bearbeitende Dashboard öffnen.
3. Eine vorhandene Karte auf dem Dashboard kann durch Auswahl von „Bearbeiten“ im Aktionsmenü der Karte geändert werden.
4. Eine neue Karte kann zum Dashboard hinzugefügt werden, indem **Karte hinzufügen** ausgewählt wird.

   "Karten in der lokalen NetApp Console-Bereitstellung anpassen".

5. **Änderungen speichern** auswählen, um das Dashboard zu speichern.
   - Sie können Ihre Änderungen auch als neues Dashboard speichern, indem Sie im Aktionsmenü **Als neues Dashboard speichern** auswählen. Diese Option ist nützlich, wenn das ursprüngliche Dashboard für andere Teams oder Flotten beibehalten werden soll, während eine neue Version für die aktuellen Überwachungsanforderungen erstellt wird.
   - Sie können Ihre Änderungen auch verwerfen, indem Sie im Aktionsmenü die Option „Änderungen verwerfen“ auswählen. Diese Option ist hilfreich, wenn Sie zur zuletzt gespeicherten Version des Dashboards zurückkehren möchten.

Ein benutzerdefiniertes Dashboard für eine andere Ressource oder Flotte wiederverwenden

Ein Dashboard kann dupliziert werden, wenn ein bewährtes Layout für ein anderes Team, eine andere Flotte oder ein anderes Überwachungsszenario wiederverwendet werden soll, ohne es von Grund auf neu zu erstellen.

Sie können ein vordefiniertes Dashboard duplizieren, um eine benutzerdefinierte Version zu erstellen, die Sie bearbeiten können.

Schritte

1. **Speicher > Dashboards** auswählen.
2. Für das Dashboard, das Sie duplizieren möchten, im Aktionsmenü **Duplizieren** auswählen.

   Bei der lokalen Bereitstellung über die Console wird eine Kopie erstellt, die alle Karten des ursprünglichen Dashboards enthält.

3. Ein Name und eine Beschreibung für das duplizierte Dashboard werden bereitgestellt.
4. Wählen Sie das soeben erstellte duplizierte Dashboard aus. Die Metriken, Ressourcen und Kartentypen können an das neue Überwachungsszenario angepasst werden.

   "Karten in der lokalen NetApp Console-Bereitstellung anpassen".

Dashboards, die nicht mehr verwendet werden, entfernen

Ein Dashboard kann gelöscht werden, wenn es die aktuellen Vorgänge nicht mehr unterstützt und die Dashboard-Liste auf aktive Anwendungsfälle fokussiert bleiben soll.

Schritte

1. **Speicher > Dashboards** auswählen.
2. Für das Dashboard, das Sie entfernen möchten, **Löschen** auswählen.
3. Bestätigen Sie die Löschung.

Verwandte Informationen

- "Startseitenmetriken in der lokalen NetApp Console-Bereitstellung anzeigen"
- "Erste Schritte mit Dashboards in NetApp Console lokale Bereitstellung"
- "Informationen zu benutzerdefinierten Dashboards in der lokalen NetApp Console-Bereitstellung"
- "Ein benutzerdefiniertes Dashboard erstellen"
- "Anpassen von Dashboard-Karten in der lokalen NetApp Console-Bereitstellung"

Flotten mithilfe des Inventars in der lokalen NetApp Console-Bereitstellung überwachen

In der lokalen NetApp Console-Bereitstellung ermöglicht die Bestandsverwaltung die Überwachung des Zustands der Speicherflotte und die Untersuchung der Speicherressourcen in der Umgebung. Die Bestandsverwaltung bietet Ansichten zu Kapazität, Sicherheit und Leistung, die bei der Identifizierung von Problemen, dem Verständnis der Ressourcenauslastung und der Nachverfolgung verwalteter Speichersysteme unterstützen.

Die Inventarverwaltung dient primär der Information und Diagnose. Im Inventar können Systeme, Volumes und andere Speicherobjekte Ihrer Flotten überprüft und gängige Aktionen wie die Bereitstellung von Speicherressourcen durchgeführt werden. Für erweiterte Speicherverwaltungsoperationen leitet die lokale Bereitstellung der NetApp Console zum System Manager weiter.

Inventarzugriff

Auf **Inventar** kann in mehreren Bereichen der lokalen NetApp Console-Bereitstellung zugegriffen werden, darunter:

- Die Startseite
- Flottenübersichtsseiten
- Flottenzustandskarten und zugehörige Bestandsansichten

Je nachdem, wo Sie **Inventar** aufrufen, kann der angezeigte Umfang auf Organisationsebene oder Flottenebene liegen.

Inventaransichten

Inventory bietet verschiedene Ansichten, die bei der Analyse unterschiedlicher Aspekte Ihrer Storage-Umgebung unterstützen.

Kapazität
: Kapazitätsauslastung anzeigen und Systeme, Volumes sowie andere Speicherobjekte identifizieren, die Speicherressourcen verbrauchen.

Sicherheit
: Sicherheitsrelevante Informationen und den Compliance-Status der verwalteten Speicherressourcen einsehen.

Performance
: Leistungsbezogene Kennzahlen werden analysiert und Ressourcen identifiziert, die möglicherweise weiterer Untersuchungen bedürfen.

Die angezeigten Informationen variieren je nach ausgewählter Ansicht und Objekttyp.

Speicherressourcen untersuchen

Inventar kann verwendet werden, um:

- Flottenzustand überwachen
- Speicherkapazitätsnutzung überprüfen
- Verwaltete Speichersysteme nachverfolgen
- Volumen und andere Objekte identifizieren, die Kapazität beanspruchen
- Mögliche Sicherheits- oder Leistungsprobleme untersuchen
- Ressourcen, die administrative Aufmerksamkeit erfordern, identifizieren

Inventory unterstützt den Wechsel von einer Übersicht auf hoher Ebene über Ihre Umgebung zu einer detaillierteren Untersuchung spezifischer Speicherressourcen.

Speicherressourcen bereitstellen

Die Inventarisierung umfasst Workflows, die das Bereitstellen von Speicherressourcen wie Volumes und LUNs ermöglichen.

Bei der Bereitstellung von Ressourcen wird ein vorhandenes verwaltetes Speichersystem ausgewählt und die

für die Arbeitslast erforderlichen Konfigurationseinstellungen werden bereitgestellt.

Inventar und Benachrichtigungen

Warnmeldungen werden für bestimmte Speicherobjekte und Zustände innerhalb Ihrer Umgebung generiert.

Wenn Sie eine Warnung auswählen, kann die lokale Bereitstellung der NetApp Console Sie zum System Manager weiterleiten, um weitere Untersuchungen oder Verwaltungsmaßnahmen vorzunehmen. **Inventory** ergänzt Warnungen, indem es eine umfassendere Sicht auf den Gesamtzustand Ihrer Speicherumgebung und der verwalteten Ressourcen bietet.

Erweiterte Managementaufgaben

Inventory hilft dabei, Ressourcen zu identifizieren, die Maßnahmen erfordern, aber einige fortgeschrittene Speicherverwaltungsoperationen werden im System Manager durchgeführt.

Beispiele hierfür sind:

- Erweitertes Workload Management
- Aufgaben zur Ressourcenverlagerung und Optimierung
- Detaillierte Systemadministrationsaktivitäten

Inventory dient zur Identifizierung und Untersuchung von Problemen, während bei Bedarf weitergehender Verwaltungsfunktionen System Manager verwendet wird.

Warnmeldungen beheben

Informationen zu Warnmeldungen in der lokalen NetApp Console-Bereitstellung

NetApp Console lokale Bereitstellung generiert Warnmeldungen, die Integritätsprobleme in Ihren lokalen ONTAP Clustern sowie bei NetApp Backup and Recovery Vorgängen identifizieren.

Die lokale Bereitstellung der Console konsolidiert Warnmeldungen von ONTAP Clustern und Backup and Recovery Vorgängen in einer einzigen Ansicht. Die Seite „Warnmeldungen“ umfasst ein Dashboard, eine Warnmeldungsliste und eine Systemansicht, sodass Warnmeldungen organisationsweit oder für eine bestimmte Flotte oder ein bestimmtes System überprüft werden können. Jede Warnmeldung identifiziert das betroffene System, den Schweregrad und den Auswirkungsbereich.

Warnungen in der lokalen NetApp Console-Bereitstellung dienen dazu:

- Kapazitäts-, Verbindungs-, Datenschutz-, Leistungs- und Sicherheitsprobleme werden erkannt.
- Warnmeldungen nach Schweregrad und Auswirkungsbereich priorisieren.
- Eine Warnung im System Manager oder Workload Analyzer öffnen und anschließend eine geführte oder automatisierte Fix-It Aktion ausführen, wenn die Seite eine solche anbietet.
- Benachrichtigungen können per E-Mail an Benutzer mit festgelegten Zugriffsrollen weitergeleitet oder Alarmdaten über einen Webhook an ein externes System gesendet werden.
- Die Warnmeldungsliste kann für eine Offline-Analyse in eine CSV-Datei exportiert werden.

Schweregrad und Auswirkungsbereiche von Warnungen

Jede Warnmeldung enthält einen Schweregrad und einen Betroffenenbereich:

- **Schweregrad** gibt die Dringlichkeit an, von höchster zu niedrigster: Kritisch, Schwerwiegend, Geringfügig, Warnung und Info.
- **Auswirkungsbereich** kennzeichnet die betroffene Domäne: Kapazität, Konnektivität, Datenschutz, Leistung und Sicherheit.

Alarmquellen und Umfang

- **ONTAP Warnungen** stammen vom ONTAP Event Management System (EMS) auf den lokalen Clustern, die von der lokalen Bereitstellung der Console erkannt wurden. "Weitere Informationen zu ONTAP EMS und den verfügbaren Warnmeldungen."
- **NetApp Backup and Recovery-Warnungen** stammen aus Backup and Recovery-Aktionen."Weitere Informationen zu NetApp Backup and Recovery-Warnungen."
- Ihre Berechtigungen bestimmen, welche Flotten Sie anzeigen können. Die Ansicht kann auf die gesamte Organisation, eine bestimmte Flotte oder ein einzelnes System beschränkt werden. Die Registerkarte **Systemstatus** zeigt den Status der einzelnen Systeme an und die Registerkarte **Warnungen** zeigt die aktuelle Warnliste für den ausgewählten Bereich.
- Der CSV-Export spiegelt den aktuellen Suchbereich, den Suchtext und die Filter wider.

Regeln für Alarmbenachrichtigungen

Benachrichtigungsregeln legen fest, welche Warnmeldungen Benachrichtigungen auslösen und wer diese erhält. Eine Benachrichtigungsregel hat folgende Eigenschaften:

- Es gleicht Warnmeldungen zum Dienst (z. B. ONTAP Management oder NetApp Backup and Recovery), Schweregrad, Auswirkungsbereich und Zielsystem ab.
- Bei der E-Mail-Zustellung werden Benachrichtigungen an Benutzer mit den angegebenen Zugriffsrollen gesendet. Bei der Webhook-Zustellung werden Alarmdaten an den konfigurierten Endpunkt gesendet, der Zugriff auf diese Daten wird von der empfangenden Anwendung und nicht von der lokalen Console Bereitstellung gesteuert.
- Es gilt für bestimmte Systeme, nicht für Flotten.
- Es kann während eines geplanten Wartungsfensters stummgeschaltet werden, um erwartete Warnmeldungen zu unterdrücken.

Die lokale Bereitstellung der Console beinhaltet eine Standardbenachrichtigungsregel, die direkt nach der Installation aktiv ist. Die Standardregel überwacht alle Dienste und Systeme auf Warnmeldungen mit Schweregrad "Critical" und sendet Benachrichtigungen ausschließlich an das Console Benachrichtigungscenter, E-Mail- oder Webhook-Benachrichtigungen werden erst nach entsprechender Einrichtung konfiguriert. Diese Regel kann angezeigt und angepasst werden, zudem lassen sich benutzerdefinierte Regeln erstellen, die auf Ihre Umgebung abgestimmt sind.

Warnmeldungen der Stufe „Info“ sind auf der Warnmeldungsseite sichtbar, werden aber nicht per Benachrichtigung zugestellt, es sei denn, Sie erstellen explizit eine Regel, die den Schweregrad „Info“ enthält.

Verwandte Informationen

- "Warnmeldungen überwachen und untersuchen"
- "Alarmbenachrichtigungsregeln erstellen und verwalten"
- "Informationen zu ONTAP Warnungen in der lokalen NetApp Console-Bereitstellung"

Warnmeldungen in der lokalen NetApp Console-Bereitstellung überwachen und untersuchen

Warnmeldungen in der lokalen NetApp Console-Bereitstellung werden überwacht und untersucht, um die Speicherintegrität zu gewährleisten und Störungen zu minimieren.

Aktive Warnmeldungen im gesamten Unternehmen oder für eine bestimmte Flotte werden angezeigt, sie lassen sich nach Schweregrad und Auswirkungsbereich priorisieren und die Ursachen können untersucht werden, sodass Probleme behoben werden, bevor sie sich verschärfen. Wenn eine Warnmeldung eine empfohlene Maßnahme oder eine Fix It-Option enthält, ist ein direkter Übergang von der Untersuchung zur Behebung möglich.

Erforderliche Zugriffsrolle

Alle Rollen außer Federation admin und Federation viewer. Benutzer mit der Rolle Federation admin oder Federation viewer können keine Warnmeldungen anzeigen. "Informationen zu Zugriffsrollen".

Für ONTAP-Warnmeldungen stehen Tools wie System Manager und Workload Analyzer direkt auf der Warnmeldungsseite zur Verfügung, um Probleme zu untersuchen und zu beheben.

Für externe Berichte kann die Warnmeldungsliste zur Offline-Analyse in eine CSV-Datei exportiert werden.

Sie können auch Benachrichtigungsregeln einrichten, um Benachrichtigungen per E-Mail oder Webhook zu erhalten. "Informationen zum Einrichten von Benachrichtigungen".

Verfügbare Benachrichtigungen

NetApp Console lokale Bereitstellung unterstützt Warnmeldungen für ONTAP und NetApp Backup and Recovery.

- "Informationen zu ONTAP Warnungen in der lokalen NetApp Console-Bereitstellung"
- "Weitere Informationen zu NetApp Backup and Recovery-Warnungen."

Benachrichtigungsdashboard anzeigen

Über das Warnmeldungs-Dashboard erhalten Sie einen schnellen Überblick über die aktuelle Warnmeldungsaktivität im ausgewählten Bereich. Das Dashboard fasst aktive Warnmeldungen nach Schweregrad und Auswirkungsbereich zusammen und enthält ein Diagramm, das die Warnmeldungsverteilung der letzten 24 Stunden darstellt, sodass Trends schnell erkannt werden können.

Das Dashboard kann gefiltert werden, um kritische Warnmeldungen oder Warnmeldungen für einen bestimmten Wirkungsbereich anzuzeigen.

Schritte

1. **Health > Warnungen > Übersicht** auswählen.
2. Im Bereichsauswahlmenü kann eine der folgenden Optionen ausgewählt werden:
   - **Alle** (Standardeinstellung), um Benachrichtigungen für alle Flotten anzuzeigen, auf die Sie Zugriff haben
   - Eine bestimmte Flotte, für die nur Warnmeldungen für diese Flotte angezeigt werden
3. Das Dashboard kann nach den Benachrichtigungen gefiltert werden, die angezeigt werden sollen, einschließlich:
   - Schweregrad (Kritisch, Warnung oder Information)

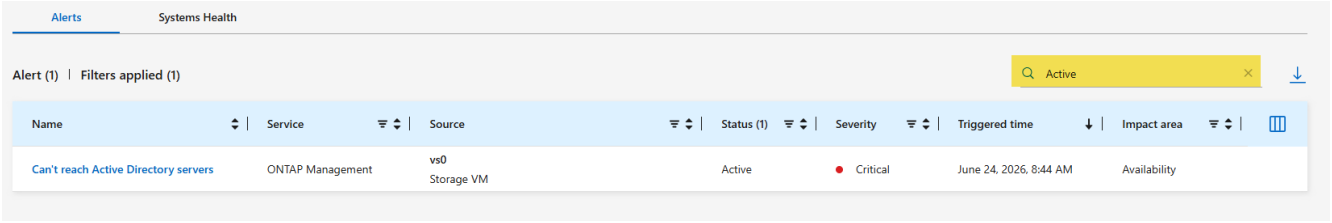
- Kritische Warnmeldungen, gruppiert nach Wirkungsbereich
- Wirkungsbereich (Sicherheit, Schutz, Verfügbarkeit, Leistung, Kapazität oder Konfiguration)

Alle Benachrichtigungen anzeigen

Über die Registerkarte „Warnungen“ wird die vollständige Liste der aktiven Warnungen für den ausgewählten Bereich angezeigt. Die Liste wird entsprechend dem aktuellen Organisations- oder Flottenbereich aktualisiert, und die Liste kann nach bestimmten Warnungen anhand des Namens oder der Beschreibung durchsucht werden.

Schritte

1. **Health > Warnungen > Übersicht** auswählen.
2. Im Bereichsauswahlmenü kann eine der folgenden Optionen ausgewählt werden:
   - **Alle** (Standardeinstellung), um Benachrichtigungen für alle Flotten anzuzeigen, auf die Sie Zugriff haben
   - Eine bestimmte Flotte, für die nur Warnmeldungen für diese Flotte angezeigt werden
3. Die Registerkarte **Warnungen** zeigt die vollständige Liste der aktiven Warnungen für den ausgewählten Bereich an.
4. Optional kann die Liste nach Name oder Beschreibung nach einer bestimmten Benachrichtigung durchsucht werden.



Benachrichtigungen nach System anzeigen

Sie können Warnmeldungen für ein bestimmtes System innerhalb einer Flotte oder Ihrer Organisation anzeigen.

Schritte

1. **Health > Warnungen > Übersicht** auswählen.
2. Im Bereichsauswahlmenü kann eine der folgenden Optionen ausgewählt werden:
   - **Alle** (Standardeinstellung), um Benachrichtigungen für alle Flotten anzuzeigen, auf die Sie Zugriff haben
   - Eine bestimmte Flotte, für die nur Warnmeldungen für diese Flotte angezeigt werden
3. Die Registerkarte **Systemzustand** zeigt eine Zusammenfassung der Warnungen an, die den Systemen innerhalb des ausgewählten Bereichs zugeordnet sind.
4. **Warnungen anzeigen** in der Zeile des jeweiligen Systems auswählen, um die vollständige Liste der aktiven Warnungen zu sehen, die diesem System zugeordnet sind.

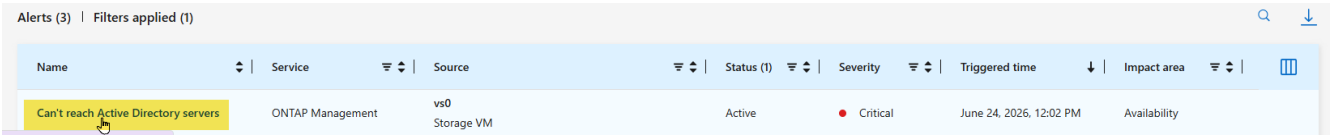
Eine Warnmeldung untersuchen

Sie können eine Warnmeldung untersuchen, um herauszufinden, was sie ausgelöst hat und wer die Benachrichtigung erhalten hat.

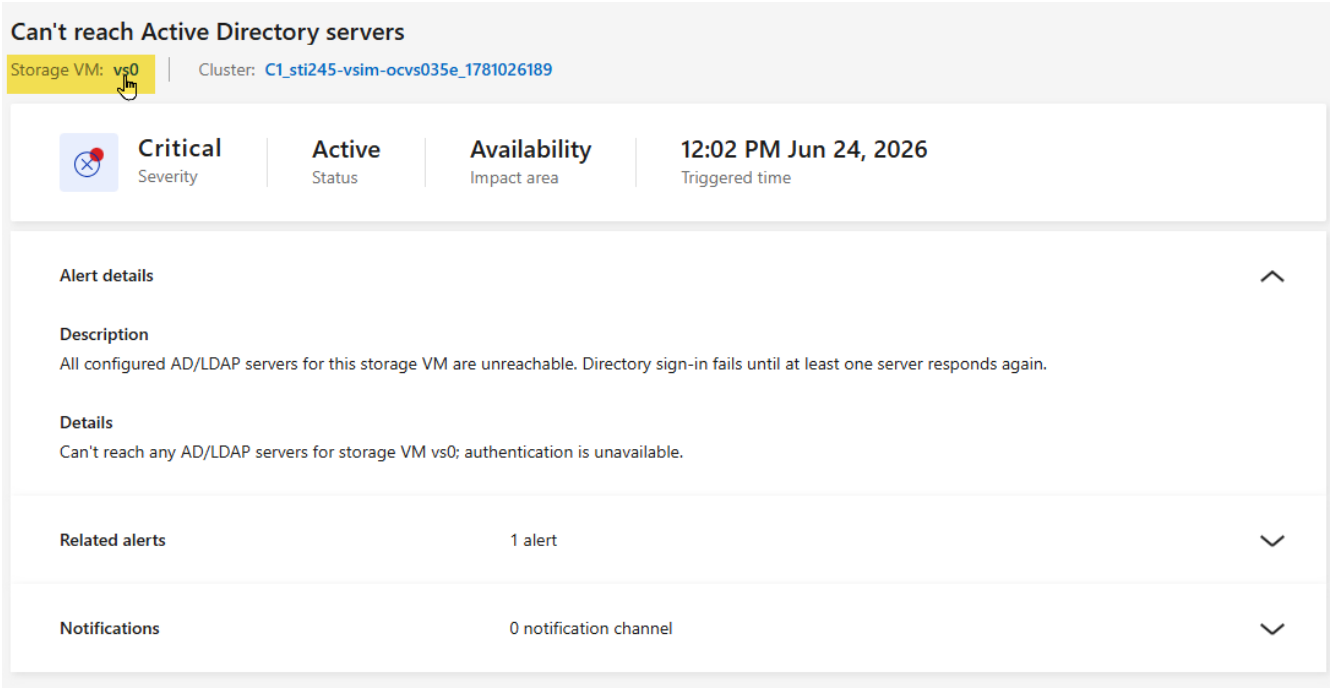
Bei der Untersuchung einer ONTAP-Warnung ist es auch möglich, direkt zur System Manager Oberfläche des Systems zu wechseln, das die Warnung ausgelöst hat, um weitere Details anzuzeigen und Maßnahmen zu ergreifen.

Schritte

1. **Health > Warnungen > Übersicht** auswählen.
2. Im Bereichsauswahlmenü kann eine der folgenden Optionen ausgewählt werden:
   - **Alle** (Standardeinstellung), um Benachrichtigungen für alle Flotten anzuzeigen, auf die Sie Zugriff haben
   - Eine bestimmte Flotte, für die nur Warnmeldungen für diese Flotte angezeigt werden
3. In einem der beiden Tabs kann der Name der Warnung ausgewählt werden, die untersucht werden soll, um die Details anzuzeigen.



4. Gegebenenfalls kann der VM- oder Clustername ausgewählt werden, um die System Manager Oberfläche für das System zu öffnen, das die Warnung generiert hat.



Eine Warnung beheben

Wenn eine Warnmeldung eine empfohlene Aktion oder eine Fix It-Option enthält, kann damit direkt von der Untersuchung zur Behebung übergegangen werden, ohne die Warnmeldungsdetails zu verlassen.

Schritte

1. **Health > Warnungen > Übersicht** auswählen.
2. Im Bereichsauswahlmenü kann eine der folgenden Optionen ausgewählt werden:
   - **Alle** (Standardeinstellung), um Benachrichtigungen für alle Flotten anzuzeigen, auf die Sie Zugriff

haben

- Eine bestimmte Flotte, für die nur Warnmeldungen für diese Flotte angezeigt werden

3. Wählen Sie die Warnung aus, die behoben werden soll.
4. Die Details der Warnmeldung können geprüft und anschließend die empfohlene Aktion oder die Option **Problem beheben** ausgewählt werden, falls eine solche verfügbar ist.
5. Führen Sie die geführten Schritte aus, um die Korrekturmaßnahme anzuwenden, und kehren Sie dann zu den Alarmdetails zurück, um den Alarmstatus zu bestätigen.

Wenn die Maßnahme das Problem behebt, erscheint die Warnung für diesen Bereich nicht mehr als aktiv. Wenn die Warnung weiterhin aktiv ist, sollten die Warnungsdetails erneut überprüft und die Untersuchung fortgesetzt werden.

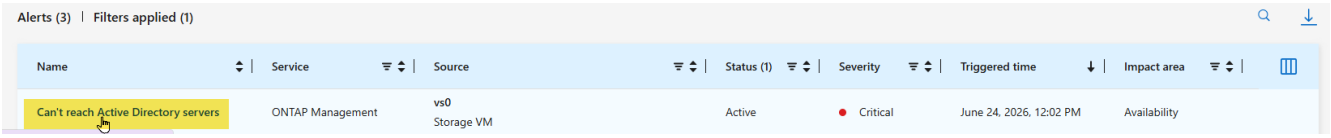
Eine Warnmeldung analysieren

Eine ONTAP Warnung kann im Workload Analyzer analysiert werden, um nachzuvollziehen, was sie ausgelöst hat.

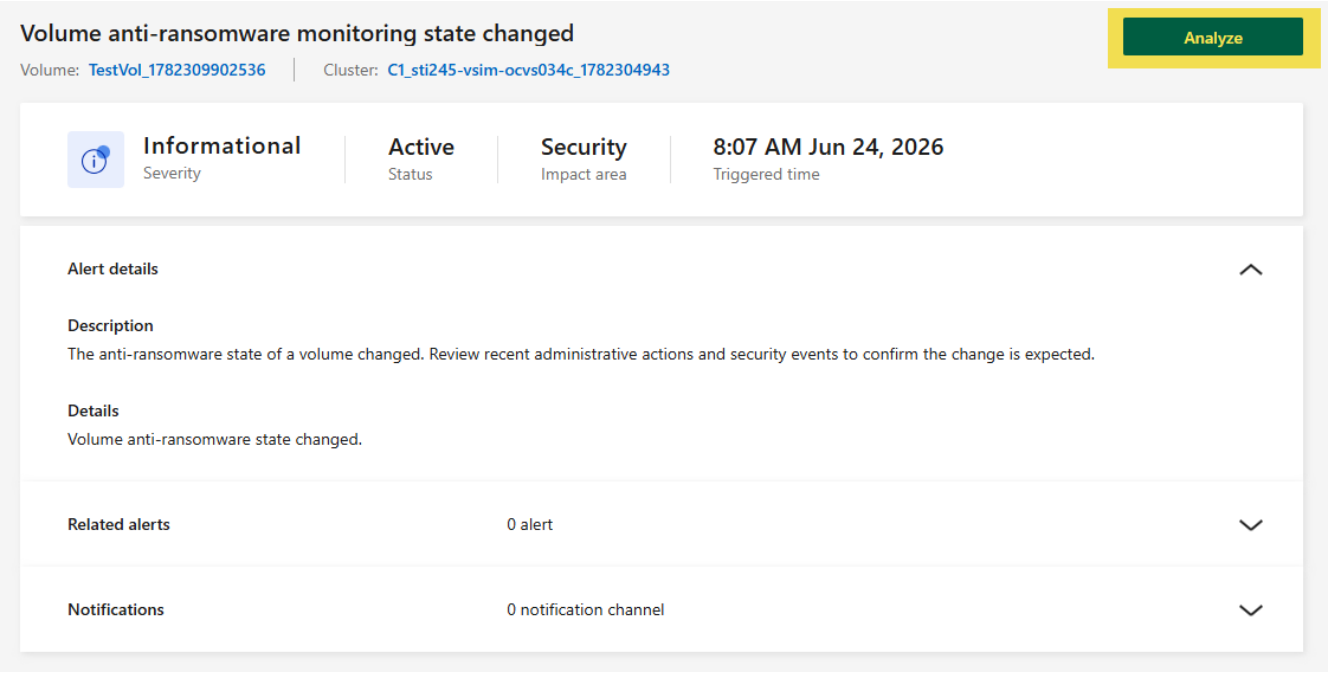
Bei der Untersuchung einer ONTAP-Warnung ist es auch möglich, direkt zur System Manager Oberfläche des Systems zu wechseln, das die Warnung ausgelöst hat, um weitere Details anzuzeigen und Maßnahmen zu ergreifen.

Schritte

1. **Health > Warnungen > Übersicht** auswählen.
2. Im Bereichsauswahlmenü kann eine der folgenden Optionen ausgewählt werden:
   - **Alle** (Standardeinstellung), um Benachrichtigungen für alle Flotten anzuzeigen, auf die Sie Zugriff haben
   - Eine bestimmte Flotte, für die nur Warnmeldungen für diese Flotte angezeigt werden
3. Die Registerkarte **Systemzustand** zeigt die vollständige Liste der aktiven Warnungen für den ausgewählten Bereich an.
4. In einem der beiden Tabs kann der Name der Warnung ausgewählt werden, die untersucht werden soll, um die Details anzuzeigen.



5. Gegebenenfalls kann **Analysieren** ausgewählt werden, um die Workload Analyzer Oberfläche für das System zu öffnen, das die Warnung generiert hat.



6. Geben Sie den Zeitraum ein, in dem die Warnung ausgelöst wurde, und wählen Sie dann **Analysieren**, um die Analyseergebnisse anzuzeigen. "Informationen zu Workload Analyzer."

Benachrichtigungen als CSV exportieren

Die Warnmeldungenliste in der lokalen NetApp Console-Bereitstellung kann für eine Offline-Analyse oder Berichterstellung in eine CSV-Datei exportiert werden. Der Export spiegelt den aktuellen Geltungsbereich (Organisation oder Flotte), den Suchtext und die Filter wider.

Schritte

1. Wählen Sie **Health > Warnungen** und dann die Registerkarte **Warnungen** aus.
2. Den Umfang (Organisation oder Flotte) festlegen und alle gewünschten Filter oder Suchtexte anwenden, die in den Export einbezogen werden sollen.
3. Das Download-Symbol ermöglicht den Export der Warnmeldungsliste in eine CSV-Datei.

Benachrichtigungsregeln für Warnungen in der lokalen NetApp Console-Bereitstellung konfigurieren

Benachrichtigungsregeln in der lokalen Bereitstellung der NetApp Console konfigurieren, um zu steuern, welche Warnungen Benachrichtigungen auslösen, wer sie erhält und wie sie zugestellt werden.

Erforderliche Zugriffsrollen

Superadministrator, Organisationsadministrator, Speicheradministrator, Analyst für Betriebssupport oder eine der Administratorrollen für NetApp Backup and Recovery. "Informationen zu Zugriffsrollen".

Benachrichtigungsregeln ermöglichen das Weiterleiten der passenden Warnmeldungen über die für Ihre Umgebung geeigneten Kanäle an die richtigen Personen, während gleichzeitig die Anzahl nicht relevanter Warnmeldungen reduziert wird. Benachrichtigungsregeln ergänzen die Alerts-Seite: Die Warnmeldung wird im Alerts-Workflow untersucht oder behoben, anschließend lässt sich mit Regeln steuern, wie ähnliche Warnmeldungen künftig zugestellt werden.

Eine Benachrichtigungsregel ordnet Warnmeldungen anhand von Bedingungen zu, die Sie definieren, wie

Dienst, Schweregrad und Auswirkungsbereich, und sendet anschließend eine Benachrichtigung über die von Ihnen ausgewählten Kanäle. Die lokale Bereitstellung der Console enthält Standard-Benachrichtigungsregeln, die angezeigt und angepasst werden können, und es besteht die Möglichkeit, eigene benutzerdefinierte Regeln zu erstellen. Regeln können auch stummgeschaltet werden, um Benachrichtigungen während geplanter Ereignisse wie Wartungsfenster vorübergehend zu unterdrücken.

- "Weitere Informationen zu ONTAP EMS und den verfügbaren Warnmeldungen."

Bevor Sie beginnen

- Damit Benachrichtigungen per E-Mail zugestellt werden, muss Ihr Organisationsadministrator einen E-Mail-Server in der lokalen NetApp Console-Bereitstellung konfigurieren. Damit Benachrichtigungen an ein externes System zugestellt werden, muss Ihr Organisationsadministrator einen Webhook konfigurieren. Die Schritte sind unter "Benachrichtigungszustellung konfigurieren" zu finden.
- Das Benachrichtigungscenter der lokalen NetApp Console-Bereitstellung zeigt Benachrichtigungen standardmäßig an, sodass für Benachrichtigungen in der NetApp Console keine zusätzliche Einrichtung erforderlich ist.

Benachrichtigungsregeln anzeigen

Die Seite mit den Benachrichtigungsregeln ist der zentrale Ort, um alle für Ihre Organisation geltenden Regeln einzusehen und zu verwalten. Jede Regel zeigt ihre wichtigsten Attribute an, sodass Sie Ihr Benachrichtigungsverhalten schnell beurteilen und anpassen können.

Schritte

1. In der linken Navigation **Health > Alerts** auswählen.
2. **Benachrichtigungseinstellungen** auswählen.
3. Überprüfen Sie die Regeln in der Liste. Jede Regel zeigt ihren aktiven Status, ihren Namen, die überwachten Dienste und Schweregrade, die Rollen, die zum Empfang von Benachrichtigungen berechtigt sind, die aktivierten Zustellungskanäle, das Datum der letzten Änderung und einen eventuell geplanten Stummschaltungszeitraum an.
4. Um eine bestimmte Regel zu finden, können die Filter- und Suchsteuerelemente verwendet werden, um nach aktivem Status, Dienst, Schweregrad, Rolle, Kanal oder Stummschaltungsstatus zu filtern.

Eine Benachrichtigungsregel erstellen

Erstellen Sie eine Benachrichtigungsregel, um die Bedingungen zu definieren, die eine Benachrichtigung auslösen, und wie diese Benachrichtigung zugestellt wird.

> Benachrichtigungsregeln lassen sich nicht für Flotten festlegen. Sie können nur für einzelne Systeme festgelegt werden. In großen Umgebungen mit vielen Systemen empfiehlt sich die Erstellung allgemeinerer Regeln nach Schweregrad, anstatt Regeln für jedes System einzeln zu duplizieren. Beispielsweise dient eine einzige Regel für den Schweregrad „Kritisch“, die alle Systeme abdeckt, als Auffangregel, ergänzt durch gezielte Regeln für Systeme, die ein anderes Routing oder andere Empfänger benötigen.

Beispiel einer Benachrichtigungsregel für kritische Warnmeldungen in allen Systemen

Angenommen, Sie möchten sicherstellen, dass keine kritische Warnung unbemerkt bleibt, unabhängig vom System, aus dem sie stammt. Es kann eine allgemeine Regel erstellt werden, die alle kritischen Warnungen an das Console Notification Center für Speicheradministratoren weiterleitet.

In diesem Beispiel wird eine Regel mit den folgenden Einstellungen erstellt:

- **Services**: Alle
- **Schweregrad**: Kritisch
- **IAM role**: Storage-Administrator
- **System**: (Dieses Feld leer lassen, um auf alle Systeme anzuwenden)
- **Übermittlungsmethode**: Konsolenbenachrichtigungszentrum

Mit dieser Regel erhalten Speicheradministratoren in der NetApp Console eine Benachrichtigung für jede kritische Warnung in allen Systemen. Diese Regel dient als Grundlage, die durch gezieltere Regeln ergänzt werden kann.

Beispiel einer gezielten Benachrichtigungsregel für Storage-Admin-Kapazitätswarnungen

Angenommen, Ihre Speicheradministratoren müssen umgehend auf kritische Kapazitätsprobleme eines bestimmten Produktionssystems reagieren, aber Sie möchten nicht, dass ihre Postfächer mit Warnmeldungen mit niedrigerem Schweregrad überflutet werden. Es kann eine gezielte Regel erstellt werden, die Speicheradministratoren nur dann per E-Mail benachrichtigt, wenn eine kritische Kapazitätswarnung für dieses System ausgelöst wird.

In diesem Beispiel wird eine Regel mit den folgenden Einstellungen erstellt:

- **Services**: ONTAP Management
- **Schweregrad**: Kritisch
- **Auswirkungsbereich**: Kapazität
- **IAM role**: Storage-Administrator
- **System**: <system_name>
- **Zustellungsmethode**: E-Mail

Mit dieser Regel sendet Console local deployment allen Speicheradministratoren des angegebenen Systems eine E-Mail, wenn eine kritische Kapazitätswarnung auftritt. Warnungen mit einem niedrigeren Schweregrad, wie beispielsweise Warnungen oder Informationen, generieren keine E-Mail, sodass sich das Team auf die Probleme konzentrieren kann, die dringend Aufmerksamkeit erfordern.

Schritte

1. In der linken Navigation **Health > Alerts** auswählen.
2. **Benachrichtigungseinstellungen** auswählen und dann **Regel hinzufügen** auswählen.
3. Definieren Sie die Bedingungen, auf die die Regel zutrifft:
    - **Regelname**: Geben Sie einen kurzen, aussagekräftigen Namen ein. Dieses Feld ist erforderlich.
    - **Regelbeschreibung**: Optional kann zusätzlicher Kontext zum Zweck der Regel eingegeben werden.
    - **Dienste**: Es kann ein oder mehrere ONTAP oder Plattformdienste ausgewählt werden, auf die die Regel angewendet wird.
    - **Rollen**: Die Zugriffsrollen, die Benutzer haben müssen, um Benachrichtigungen zu erhalten, wenn die Regel ausgelöst wird, können ausgewählt werden.
    - **Schweregrade**: Es kann ausgewählt werden, welche Schweregrade die Regel überwacht, wie zum Beispiel Kritisch, Warnung, Fehler oder Information.
    - **Wirkungsbereich**: die passenden Betriebsbereiche wie Kapazität oder Leistung auswählen.
    - **Alarmname**: Es werden die spezifischen Alarmtypen ausgewählt, die die Regel auslösen.

- **System**: Wählen Sie den Systemkontext aus, auf den die Regel angewendet wird.

4. Wählen Sie die Zustellungskanäle für die Benachrichtigung aus:
   - **E-Mail**: Sendet Benachrichtigungs-E-Mails an Benutzer mit den ausgewählten Rollen. Erfordert einen konfigurierten E-Mail-Server.
   - **Webhook**: Sendet Alarmdaten an ein externes System. Erfordert die Auswahl einer konfigurierten Webhook-Integration.
   - **Konsolenbenachrichtigungszentrum**: Zeigt Echtzeitwarnungen für Benutzer mit den ausgewählten Rollen an.
5. Optional kann die Benachrichtigung dieser Regel während eines geplanten Zeitraums, wie zum Beispiel eines Wartungsfensters, unterdrückt werden, indem ein Zeitplan für **Benachrichtigungen stummschalten** festgelegt und eine Wiederholung ausgewählt wird, falls der Stummschaltungszeitraum wiederholt werden soll. Mehrere Stummschaltungsfenster können pro Regel hinzugefügt werden, was für wiederkehrende Wartungszyklen wie wöchentliche Patches nützlich ist.
6. **Erstellen** auswählen.

Aktivieren oder Deaktivieren einer Benachrichtigungsregel

Aktivieren oder deaktivieren Sie einzelne Benachrichtigungsregeln, um festzulegen, unter welchen Bedingungen Benachrichtigungen ausgelöst werden. Regeln, die für Ihre Umgebung nicht relevant sind, können deaktiviert werden, um die Anzahl der Benachrichtigungen zu reduzieren. Regeln können wieder aktiviert werden, um deren Benachrichtigungen erneut zu erhalten.

Schritte

1. In der linken Navigation **Health > Alerts** auswählen.
2. **Benachrichtigungseinstellungen** auswählen.
3. Suchen Sie die Regel, die geändert werden soll.
4. Den **Aktiv**-Schalter der Regel ein- oder ausschalten. Die Änderung wird sofort wirksam.

Benachrichtigungsregel stummschalten

Eine Benachrichtigungsregel kann stummgeschaltet werden, um die Zustellung von Warnungen während eines geplanten Ereignisses, wie eines Wartungsfensters, zu unterdrücken, ohne die Regel zu deaktivieren. Warnungen werden während der Stummschaltung weiterhin auf der Seite „Warnungen“ angezeigt, nur die E-Mail-, Webhook- und In-Console-Benachrichtigungen werden unterdrückt. Nach Ablauf des Stummschaltungszeitraums werden die Benachrichtigungen automatisch wieder aufgenommen.

Sie können einer einzelnen Regel mehrere Stummschaltungsfenster hinzufügen und jedes einzelne so konfigurieren, dass es nach einem Zeitplan wiederholt wird.

Beispiele für stumme Fenster

- **Einmaliges Wartungsfenster**: Sie führen am Samstagabend ein Firmware-Upgrade auf einem Speichersystem durch und möchten die erwarteten Benachrichtigungen während dieses Wartungsfensters unterdrücken. Ein Stummschaltungsfenster wird für Samstag von 22:00 Uhr bis Sonntag 2:00 Uhr ohne Wiederholung festgelegt. Nach Ablauf des Fensters werden die Benachrichtigungen automatisch wieder aufgenommen.
- **Wöchentlich wiederkehrendes Patch-Fenster**: Ihr Team patcht die Systeme jeden Sonntag von Mitternacht bis 4:00 Uhr. Ein Stummschaltungsfenster mit wöchentlicher Wiederholung sorgt dafür, dass Benachrichtigungen jede Woche automatisch ohne manuelle Eingriffe unterdrückt werden. Wenn ein zweites System einen eigenen Patch-Zeitplan zu einer anderen Zeit hat, kann derselben Regel ein zweites Stummschaltungsfenster mit eigener Startzeit und Wiederholung hinzugefügt werden.

Schritte

1. In der linken Navigation **Health > Alerts** auswählen.
2. **Benachrichtigungsregeln** auswählen.
3. In der Regelliste die Regel suchen, die stummgeschaltet werden soll, und das Aktionsmenü für diese Regel auswählen.
4. **Bearbeiten** auswählen.
5. Im Abschnitt **Benachrichtigungen stummschalten** das Start- und Enddatum sowie die Uhrzeit für das Stummschaltungsfenster festlegen.
6. Optional kann eine Wiederholung ausgewählt werden, um das Fenster nach einem Zeitplan zu wiederholen.
7. Zum Hinzufügen weiterer Stummschaltfenster **Stummschaltfenster hinzufügen** auswählen und die vorherigen Schritte wiederholen.
8. **Speichern** auswählen.

Löschen einer Benachrichtigungsregel

Löschen Sie eine Benachrichtigungsregel, wenn Sie sie nicht mehr benötigen. Durch das Löschen einer Regel wird diese endgültig entfernt, sodass sie nicht wiederhergestellt werden kann.

Schritte

1. In der linken Navigation **Health > Alerts** auswählen.
2. **Benachrichtigungseinstellungen** auswählen.
3. In der Regelliste die Regel suchen, die gelöscht werden soll, und das Aktionsmenü für diese Regel auswählen.
4. Im Aktionsmenü die Option **Löschen** auswählen.

Verwandte Informationen

- "Benachrichtigungszustellung konfigurieren"
- "Informationen zu Konsolenwarnungen"
- "Benachrichtigungen anzeigen"

Behebung von Speicherklassenabweichungen in der lokalen NetApp Console-Bereitstellung

In der lokalen Bereitstellung der NetApp Console lassen sich driftbezogene Warnmeldungen finden, Drift-Ergebnisse analysieren und Workloads beheben, die nicht mehr ihrer Speicherklassenabsicht entsprechen.

Erforderliche Rollen

Speicheradministrator

> Arbeitslasten in Flotten können nur angezeigt und behoben werden, wenn die entsprechende Berechtigung vorliegt.

Abweichungen beheben

Wenn eine Arbeitslast nicht mehr der vorgesehenen Speicherklasse entspricht, löst die lokale NetApp Console

Bereitstellung eine Warnung aus. Mit der Warnung lässt sich die Abweichung analysieren und die empfohlene Behebung anwenden.

Einige Korrekturmaßnahmen lassen sich direkt aus der Warnmeldung anwenden. Für andere Probleme empfiehlt sich eine Aktualisierung der Workload-Konfiguration oder die Zuweisung einer anderen Speicherklasse, um die Compliance wiederherzustellen. Der Korrektur-Workflow zeigt die erwarteten Auswirkungen an, bevor Änderungen vorgenommen werden.

Schritte

1. **Speicher > Speicherklassen** auswählen.

   Eine Zusammenfassung der Speicherklassenabweichungen erscheint im Bereich **Abweichungen nach Speicherklasse**. Die vollständige Liste erscheint in der Tabelle.

2. In der Spalte **Drifts** die Option **View** für die relevante Speicherklasse auswählen.

   Die Seite **Benachrichtigungen > Übersicht** wird mit angewendeten Filtern geöffnet.

3. Eine Warnung kann ausgewählt werden, um die Seite mit den Warnungsdetails zu öffnen.
4. **Analysieren** auswählen.
5. Die Ergebnisse im **Workload analyzer** werden angezeigt.

   Bei Feststellungen zur Konfigurationsabweichung werden die Soll- und Ist-Einstellungen verglichen, um zu bestimmen, was sich geändert hat.

6. Wählen Sie die empfohlene Abhilfemaßnahme, wie zum Beispiel **Beheben**.
7. Die vorgeschlagenen Änderungen und die Abhilfemaßnahmen können überprüft und angewendet werden.
8. Zurück zu **Speicher > Speicherklassen** und prüfen, ob die Arbeitslast nicht mehr als verschoben angezeigt wird.

   Die Überprüfung der Konformität kann einige Minuten dauern, bis die kürzlich vorgenommenen Konfigurationsänderungen berücksichtigt sind. Wenn die Arbeitslast weiterhin als abweichend aufgeführt ist, zur Seite mit den Warnungsdetails zurückkehren und **Analysieren** auswählen, um verbleibende Ergebnisse zu überprüfen.

Verwandte Informationen

- "Informationen zu Speicherklassenabweichungen und Compliance in der lokalen Bereitstellung der NetApp Console"
- "Informationen zu Speicherwarnungen"
- "Benachrichtigungen anzeigen"

Maßnahmen zur Behebung von Warnungen in der lokalen NetApp Console-Bereitstellung

Diese Referenz dient dem Verständnis der in **Fix it** in der lokalen NetApp Console-Bereitstellung verfügbaren Korrekturmaßnahmen. Für jede Aktion beschreibt die Tabelle, was die Aktion bewirkt und die zugehörige Warnung. Die Aktionsdetails im Bestätigungsdialog sollten vor der Ausführung überprüft werden.

Abhilfemaßnahmen

Abhilfemaßnahme	Alarmname	Alarmbeschreibung	Wirkungsbereich	Zusammenfassung der Sanierungsmaßnahmen
Automatisches Volumenwachstum aktivieren	Volume voll	Das Volume hat nur noch wenig freien Speicherplatz und nähert sich der vollen Kapazität.	Kapazität	Erhöht automatisch die Größe eines Volumes (bis zu einem konfigurierten Grenzwert), um das Risiko eines Speicherplatzmangels zu verringern.
Volumengröße ändern	Volume voll	Das Volume hat nur noch wenig freien Speicherplatz und nähert sich der vollen Kapazität.	Kapazität	Erhöht die Größe eines Volumes, um sofort mehr Speicherplatz bereitzustellen.
Volume online schalten	Volume offline	Das Volume ist offline und stellt keine Daten bereit.	Verfügbarkeit	Bringt ein Offline-Volume online, sodass es die Datenbereitstellung wieder aufnehmen kann.
Aggregat online schalten	Offline-Aggregat	Das Aggregat ist nicht online und die darauf gehosteten Volumes sind möglicherweise nicht verfügbar.	Verfügbarkeit	Bringt ein Offline-Aggregat online, um den Zugriff auf die von ihm gehosteten Volumes wiederherzustellen.
LUN online schalten	LUN offline	Die LUN ist offline und der Hostzugriff ist nicht verfügbar.	Verfügbarkeit	Bringt eine Offline-LUN online, sodass Hosts wieder Zugriff und E/A durchführen können.
Volume entsperren	Volume eingeschränkt	Das Volume befindet sich in einem eingeschränkten Zustand und kann E/A-Vorgänge möglicherweise nicht wie gewohnt ausführen.	Verfügbarkeit	Stellt ein eingeschränktes Volume wieder in den Online-Zustand, sodass Clients wieder darauf zugreifen können.
NVMe Namespace online schalten	NVMe Namespace ist offline	Der NVMe-Namensraum ist offline und Hostzugriff ist nicht verfügbar.	Verfügbarkeit	Bringt einen Offline-NVMe-Namensraum online, um den Hostzugriff wiederherzustellen.

Abhilfemaßnahme	Alarmname	Alarmbeschreibung	Wirkungsbereich	Zusammenfassung der Sanierungsmaßnahmen
Intercluster-LIF aktivieren	Intercluster-LIF ausgefallen	Ein Intercluster-LIF ist ausgefallen und die Kommunikation zwischen den Clustern kann beeinträchtigt sein.	Konnektivität	Aktiviert eine Intercluster-LIF, um die für die Replikation verwendete Cluster-zu-Cluster-Konnektivität wiederherzustellen.
MetroCluster AUSO erneut aktivieren	MetroCluster automatische ungeplante Umschaltung deaktiviert	Die automatische ungeplante Umschaltung ist auf diesem Cluster deaktiviert.	Verfügbarkeit	Aktiviert die automatische ungeplante Umschaltung (AUSO) wieder, damit der MetroCluster Schutz wie vorgesehen funktioniert.
Service Processor Netzwerk konfigurieren	Service Processor ist nicht konfiguriert.	Das Service Processor (SP) Netzwerk ist nicht konfiguriert.	Verwaltbarkeit	Konfiguriert die SP Netzwerkeinstellungen, um den Zugriff auf das Out-of-Band-Management zu ermöglichen.
Nicht zugewiesene Datenträger zuweisen	Nicht zugewiesene Datenträger erkannt	Es sind nicht zugewiesene Datenträger vorhanden, deren Kapazität möglicherweise ungenutzt ist. Die Datenträger sollten einem Knoten zugewiesen werden, damit sie für die Speicherung verwendet werden können.	Verfügbarkeit	Weist derzeit nicht zugewiesene Datenträger einem Knoten zu, damit diese für die Speicherung verwendet werden können.
Wiederherstellung des Speicherplatzes im Root-Volume	Root-Volume-Speicherplatz des Knotens niedrig	Der verfügbare Speicherplatz auf dem Root-Volume des Knotens ist gering und kann den normalen Systembetrieb beeinträchtigen.	Systemgesundheit	Gibt Speicherplatz auf dem Root-Volume des Knotens frei, indem der größte Snapshot oder die größte Core-Dump-Datei gelöscht wird. Löschvorgänge sind dauerhaft.

Leistungsprobleme untersuchen

Informationen zum Workload Analyzer für die lokale Bereitstellung der NetApp Console

Mit dem Workload Analyzer für lokale Bereitstellungen der NetApp Console lässt sich das Verhalten eines einzelnen Volumes im Zeitverlauf anzeigen. Leistungsbeeinträchtigungen, Kapazitätstrends und Ressourcenkonflikte können direkt vom Volume, aus einer Warnmeldung oder aus dem Inventar untersucht werden.

Wie der Workload Analyzer die Hauptursachen identifiziert

Mit dem Workload Analyzer lassen sich Metriken eines einzelnen Volumes über sechs Abschnitte korrelieren, sodass die Ursachen schnell identifiziert werden können. Ein Volume und einen Zeitraum auswählen, um Ereignisse, Performance und Kapazität gemeinsam im selben Fenster anzuzeigen. Diese Ansicht kann dabei unterstützen zu bestimmen, ob der Storage die wahrscheinliche Quelle eines Applikationsproblems ist oder ob eine andere Ebene, wie etwa das Netzwerk, die Ursache darstellt.

Der Analysator ist besonders nützlich, wenn bereits bekannt ist, welches Volume betroffen ist. Wird er über eine Warnung oder aus der Volume-Inventarisierung geöffnet, öffnet Console local deployment den Analysator mit dem ausgewählten Volume, sodass der Fokus auf dem Analysefenster und den Diagrammen liegt.

Der Analysator verfolgt jeweils nur ein Volume, daher eignet er sich zur Untersuchung eines bestimmten Problems und nicht zum Vergleich mehrerer Volumes.

Der Abschnitt zur Kapazität sollte im Rahmen dieser Bewertung betrachtet werden. Wenn ein ONTAP System zu mehr als 85 % voll ist, kann die hohe Auslastung selbst Leistungsprobleme verursachen, sodass eine geringe verfügbare Kapazität Latenzzeiten erklären kann, die allein durch die Leistungsdiagramme nicht erklärt werden.

Nachdem die Ursache identifiziert wurde, ist direkt aus dem Analyzer eine Aktion möglich. Wenn automatisierte Optionen verfügbar sind, stellt die Console lokale Bereitstellung Fix-It-Empfehlungen mit geführten Schritten oder Ein-Klick-Problembehebung bereit.

Workload-Diagramme für LUNs bieten nicht den gleichen Detaillierungsgrad wie die Diagramme für Volumes, daher werden bei der Analyse einer LUN weniger Statistiken angezeigt.

Workload Analyzer aufrufen

Der Workload Analyzer kann auf verschiedene Arten geöffnet werden:

- Im Menü **Health** die Option **Workload Analyzer** auswählen, dann im Feld **Volume** nach dem Volume suchen und das gewünschte Volume zur Untersuchung auswählen.
- Auf der Seite **Speicher > Flotten > Inventar** zu einem Volume navigieren, das analysiert werden soll, und im Aktionsmenü **Analysieren** auswählen.
- Auf der Seite **Warnungen > Übersicht** eine Warnung für das Volumen auswählen, das untersucht werden soll, und dann in den Warnungsdetails **Analysieren** auswählen.

Sie können auch LUNs analysieren, aber diese zeigen weniger Statistiken als Volumes.

Latenz, Durchsatz und Speicherkapazität analysieren

Diese sechs Abschnitte dienen zur Untersuchung eines Volumes:

Volume-Auswahl

Das Volumen und den Zeitraum für die Untersuchung auswählen, sodass alle Diagramme und Ereignisse auf die gleiche Arbeitslast und das gleiche Analysefenster abgestimmt sind.

Ereigniszeitachse

Aktuelle und historische Konfigurationsänderungen, Warnmeldungen und kritische Meldungen für das ausgewählte Volume im Analysezeitraum werden angezeigt. In diesem Abschnitt lässt sich „was sich geändert hat“ mit Änderungen im Leistungs- oder Kapazitätsverhalten korrelieren.

Latenzanalyse

Die Latenz des Volumes im Zeitverlauf anzeigen, entweder als Gesamtwert oder aufgeschlüsselt nach Verzögerungszentrum (Netzwerk, Datenverarbeitung, Aggregatoperationen, Cluster-Interconnect und andere). Wenn das Volume eine QoS-Richtlinie verwendet, zeigt der Analysator die maximalen und minimalen Latenzgrenzen der Richtlinie als Referenzlinien an, sodass ersichtlich ist, wie nahe die Arbeitslast an einem Drosselungsschwellenwert liegt. Die Prognose kann umgeschaltet werden, um zu projizieren, ob die Latenz auf einen Warn- oder kritischen Schwellenwert zusteuert.

Durchsatzanalyse

IOPS und MB/s im Zeitverlauf anzeigen, optional mit einer Aufschlüsselung nach lesen/schreiben/sonstigen Zugriffen. Wenn das Volume eine QoS-Richtlinie verwendet, zeigt der Analysator IOPS- und Durchsatzbegrenzungslinien an. Die Prognose kann ein- oder ausgeblendet werden, um abzuschätzen, ob die Nachfrage sich in Richtung der QoS-Grenzwerte entwickelt.

Ressourcennutzung

Anzeigen, wie ausgelastet die Knoten und Aggregate sind, die das Volume während des Analysezeitraums bedienen. Der Analysator stellt jede Ressource als unabhängige Linie dar, anstatt Werte zu stapeln, sodass erkennbar ist, ob ein bestimmter Knoten oder ein bestimmtes Aggregat eine Quelle von Konkurrenz ist. Die Prognose kann umgeschaltet werden, um zu projizieren, ob eine Ressource auf einen Schwellenwert für hohe Auslastung zusteuert.

Kapazitätsanalyse

Anzeigen, wie sich der physische Speicherplatz und der verfügbare Speicherplatz im Volume im Laufe der Zeit verändert haben. Beim Überfahren mit dem Mauszeiger wird eine Aufschlüsselung der Speichereffizienz angezeigt, einschließlich Einsparungen durch Deduplizierung, Komprimierung und Verdichtung. Die Prognose kann umgeschaltet werden, um vorherzusagen, wann das Volume Warn- oder kritische Kapazitätsschwellenwerte erreicht. In der Snapshot-Ansicht wird angezeigt, wie sich der Snapshot-Speicherplatz im Vergleich zur konfigurierten Snapshot-Reserve entwickelt.

Prognose der Kapazitäts- und Leistungstrends

Die Prognosefunktion in jedem Analysebereich ermöglicht eine Erweiterung des Diagrammzeitraums über den aktuellen Zeitpunkt hinaus und eine Projektion zukünftiger Werte basierend auf dem beobachteten Trend. Eine gestrichelte Linie unterscheidet Prognosewerte von Ist-Daten. Der Analysator zeigt zudem eine Hinweisnachricht an, wenn die Prognose auf eine wahrscheinliche Überschreitung eines Schwellenwerts hinweist, einschließlich einer geschätzten Zeit bis zur Überschreitung.

Verwandte Informationen

"Hohe Latenz auf einem Volumen untersuchen". "Untersuchung hoher Anforderungen an den Durchsatz eines Volumes". "Kapazitätswachstum eines Volumens untersuchen". "Informationen zu den Metriken des Workload Analyzers in der lokalen NetApp Console-Bereitstellung".

Hohe Latenz auf einem Volume in der lokalen NetApp Console-Bereitstellung untersuchen

Der Workload Analyzer in der lokalen NetApp Console-Bereitstellung hilft dabei, die Ursache für die langsamen Antwortzeiten eines Volumes zu identifizieren.

Wenn der Analysator über eine Warnung oder aus der Volumenübersicht geöffnet wird, ist das Volumen bereits ausgewählt und der Fokus kann auf den Zeitbereich und die Diagrammaufschlüsselungen gelegt werden.

Wenn die Anwendungsleistung nachlässt, lässt sich ermitteln, welcher Teil des I/O-Pfads die Verlangsamung verursacht. Der Abschnitt zur Latenzanalyse unterteilt die Antwortzeit nach Verzögerungszentrum, sodass zwischen Netzwerkproblemen, Datenverarbeitungsaufwand, Aggregate-Contention und anderen

Einflussfaktoren unterschieden werden kann.

Schritte

1. Der Workload Analyzer kann mit einer der folgenden Methoden geöffnet werden:
   - Im Menü **Health** die Option **Workload Analyzer** auswählen, dann im Feld **Volume** nach dem Volume suchen und das gewünschte Volume zur Untersuchung auswählen.
   - Auf der Seite **Speicher > Flotten > Inventar** zu einem Volume navigieren, das analysiert werden soll, und im Aktionsmenü **Analysieren** auswählen.
   - Auf der Seite **Warnungen > Übersicht** eine kapazitätsbezogene Warnung für das Volume auswählen, das untersucht werden soll, dann in den Warnungsdetails **Analysieren** auswählen.
2. Den **Zeitraum** so einstellen, dass er den Zeitraum abdeckt, in dem das Leistungsproblem aufgetreten ist, dann **Analysieren** auswählen.
3. Im Abschnitt **Ereigniszeitleiste** sind Konfigurationsänderungen und Warnmeldungen zu sehen, die mit dem Anstieg der Latenzzeit übereinstimmen.

   Der Analysator stellt Konfigurationsänderungsereignisse (Schraubenschlüssel-Symbol) und Alarmereignisse (Warn- und Kritisch-Symbole) auf derselben Zeitachse wie das Latenzdiagramm dar, sodass leicht erkennbar ist, ob eine Änderung der Verschlechterung vorausging.

4. Im Abschnitt **Latenz** das Dropdown-Menü **Ansicht** öffnen und **Aufschlüsselung nach Verzögerungszentrum** auswählen. Das Diagramm zeigt den Beitrag jedes Verzögerungszentrums zur Gesamtlatenz im Zeitverlauf. Zu den Verzögerungszentren gehören:
   - Leselatenz
   - Schreiblatenz
   - Andere Latenz
5. Fahren Sie mit dem Mauszeiger über einen Punkt im Diagramm, an dem die Latenz am höchsten ist, um den Wert jedes Verzögerungszentrums und dessen prozentualen Anteil an der Gesamtlatenz zu sehen.

   Das Zentrum mit der größten Verzögerung weist in der Regel auf die Ressource hin, die am stärksten ausgelastet ist. Wenn eine gemeinsam genutzte Ressource die Nachfrage nicht decken kann, müssen die Volumes, die sie verwenden, länger auf E/A warten. Die Last auf dieser Ressource kann verringert werden, beispielsweise durch das Verschieben von Workloads oder das Anpassen eines QoS-Limits, um die Latenz zu senken.

6. Den dominanten Faktor identifizieren und den Wert zur Bestimmung der nächsten Schritte verwenden:
   - Hohe **Leselatenz** kann auf Festplatten-Contention hinweisen. Im Abschnitt **Ressourcenauslastung** lässt sich der prozentuale Anteil der Auslastung des Aggregats bestätigen.
   - Eine hohe **Schreiblatenz** kann auf eine Auslastung der Netzwerkkarte oder auf Probleme mit dem Netzwerkpfad außerhalb des Clusters hinweisen.
   - Eine hohe **sonstige Latenz** kann darauf hindeuten, dass die Inline-Effizienzeinstellungen mehr CPU-Leistung verbrauchen, als die Arbeitslast verträgt. Eine Anpassung der Effizienzeinstellungen oder von QoS kann in Betracht gezogen werden.
   - Hohe **Cloud-Latenz** kann darauf hindeuten, dass die Arbeitslast häufig auf kalte Daten in der Kapazitätsebene zugreift. Eine Anpassung der Tiering-Richtlinie kann in Betracht gezogen werden.
7. Wenn die Verzögerungszentren die Verlangsamung nicht erklären, sollte der Abschnitt **Kapazitätsanalyse** geprüft werden. Wenn das ONTAP-System zu mehr als 85 % ausgelastet ist, kann die hohe Auslastung unabhängig von der Aufschlüsselung der Verzögerungszentren zu Leistungsproblemen führen.

8. Wenn die Latenz unmittelbar nach einem Änderungsereignis anstieg, können die Ereignisdetails zusammen mit den zugehörigen Diagrammen zur Validierung der wahrscheinlichen Ursache herangezogen werden:
    - Bei Änderungen der Dienstgüte (QoS) die Latenzlinie mit den QoS-Grenzwertlinien vergleichen und die Durchsatzdiagramme prüfen, um festzustellen, ob die Nachfrage eine Richtlinienobergrenze erreicht.
    - Bei Verschiebungen von Aggregaten oder Volumes wird der Latenzanstieg mit den für denselben Zeitraum angezeigten Werten für die Auslastung von Node und Aggregat verglichen.
    - Bei Änderungen der Tiering-Richtlinie den Beitrag der Cloud-Latenz prüfen, um festzustellen, ob der Zugriff auf kalte Daten nach der Änderung zugenommen hat.

Nachdem Sie fertig sind

Wenn ein Konfigurations- oder Platzierungsproblem die Ursache des Problems ist und eine lokale Bereitstellung über die Console das Problem beheben kann, kann die Warnung auf dem Volume eine Fix-It-Option bieten.

"Informationen zu den Metriken des Workload Analyzers in der lokalen NetApp Console-Bereitstellung".

Untersuchung eines hohen Durchsatzes auf einem Volume in der lokalen NetApp Console-Bereitstellung

Mit dem Workload Analyzer in der lokalen NetApp Console-Bereitstellung lassen sich die IOPS- und Durchsatzanforderungen eines Volumes im Zeitverlauf analysieren.

Wenn die Auslastung eines Volumes mehr IOPS oder Durchsatz als erwartet benötigt, lässt sich ermitteln, was die Ursache für diesen Bedarf ist. Der Abschnitt zur Durchsatzanalyse zeigt IOPS und MB/s mit optionaler Aufschlüsselung nach Lese-, Schreib- und anderen Vorgängen, sodass erkennbar ist, welcher Typ von I/O den hohen Bedarf verursacht und ob dieser Bedarf auf ein QoS-Limit zusteuert.

Wenn der Analysator über eine Warnung oder aus der Volumeninventur geöffnet wird, ist das Volumen bereits ausgewählt und der Fokus kann auf den Zeitbereich und die Durchsatzdiagramme gelegt werden.

Schritte

1. Der Workload Analyzer kann mit einer der folgenden Methoden geöffnet werden:
    - Im Menü **Health** die Option **Workload Analyzer** auswählen, dann im Feld **Volume** nach dem Volume suchen und das gewünschte Volume zur Untersuchung auswählen.
    - Auf der Seite **Speicher > Flotten > Inventar** zu einem Volume navigieren, das analysiert werden soll, und im Aktionsmenü **Analysieren** auswählen.
    - Auf der Seite **Warnungen > Übersicht** eine Warnung für das Volumen auswählen, das untersucht werden soll, und dann in den Warnungsdetails **Analysieren** auswählen.
2. Den **Zeitraum** so einstellen, dass er den Zeitraum mit hoher Nachfrage abdeckt, dann **Analysieren** auswählen.
3. Zum Abschnitt **Durchsatzanalyse** scrollen.
4. Das Dropdown-Menü **Ansicht** öffnen und **Aufschlüsselung (RWO)** auswählen.

    Die Diagramme unterteilen sich in Lese-, Schreib- und sonstige Komponenten, sowohl für IOPS als auch für MB/s. So kann ermittelt werden, ob leseintensive Zugriffsmuster, schreibintensive Muster oder eine Kombination daraus die Nachfrage bestimmen.

5. Verwenden Sie die Komponentenauswahl, um die Metriken, die Sie untersuchen möchten, zu aktivieren oder zu deaktivieren:

- **Lese-IOPS** und **Schreib-IOPS** – Operationen pro Sekunde nach E/A-Richtung
- **Lesen MB/s** und **Schreiben MB/s** – Durchsatz in Megabyte pro Sekunde nach I/O-Richtung
- **Andere IOPS** und **Andere MB/s** (Metadaten und andere Nicht-Daten-Operationen)
- **QoS IOPS Limit** und **QoS MB/s Limit** (Richtlinienobergrenzen, die nur angezeigt werden, wenn das Volume eine QoS-Richtlinie verwendet)
- **Cloud-Durchsatz** – MB/s, die in die Cloud geschrieben und von dort gelesen werden, wird nur für Workloads angezeigt, die Kapazität über FabricPool in die Cloud auslagern

6. Fahren Sie mit dem Mauszeiger über einen Spitzenwert im Diagramm, um den genauen Wert und die prozentuale Aufschlüsselung für jede Komponente zu diesem Zeitpunkt zu sehen.

   Der Tooltip zeigt außerdem die durchschnittliche I/O-Größe (Durchsatz geteilt durch IOPS) für jede Kategorie an, was darauf hinweisen kann, ob die Arbeitslast große sequenzielle I/O-Operationen oder kleine zufällige I/O-Operationen ausführt.

7. **Prognose anzeigen** aktivieren, um abzuschätzen, ob die aktuellen Durchsatztrends die QoS-IOPS- oder MB/s-Grenze erreichen.

   Wenn sich die Prognoselinie einer QoS-Grenzlinie nähert, könnte ONTAP die Arbeitslast bald drosseln.

8. Wenn die Gesamtnachfrage ohne Aufschlüsselung angezeigt werden soll, das Dropdown-Menü **Ansicht** öffnen und **Summen** auswählen.

   Die Gesamtansicht zeigt eine einzelne IOPS-Zeile und eine einzelne MB/s-Zeile, was für eine schnelle Übersicht über den Gesamtbedarf nützlich ist.

Nachdem Sie fertig sind

Anhand der beobachteten Durchsatzmuster lässt sich bestimmen, welche nächsten Schritte sinnvoll sind:

- Wenn die Lese-IOPS im Verhältnis zu den Schreib-IOPS sehr hoch sind, kann geprüft werden, ob Vorab-Leseeinstellungen oder Caching die Last auf dem Volume reduzieren.
- Wenn sich die Arbeitslast dem QoS-IOPS- oder MB/s-Limit nähert oder dieses bereits erreicht hat, können die QoS-Limitlinien und die zugehörigen Metrikdefinitionen zur Bestätigung der Drosselung und zur Entscheidung herangezogen werden, ob eine Anpassung des Limits erforderlich ist.
- Wenn der Durchsatz hoch und die Latenz ebenfalls erhöht ist, kann im Abschnitt **Ressourcenauslastung** geprüft werden, ob der zugrunde liegende Node oder das Aggregat unter Auslastung steht. Durchsatzspitzen, Latenzspitzen und Ressourcenauslastung sollten im gleichen Zeitraum verglichen werden.
- Wenn der Analysator ein schnelles Wachstum der Kapazität oder der Snapshot-Anzahl anzeigt, während die Nachfrage steigt, sollten die Kapazitäts- und Snapshot-Metriken überprüft werden, um zu verstehen, wie sich dieses Wachstum auf das Volumen auswirken könnte.

"Hohe Latenz auf einem Volumen untersuchen". "Informationen zu den Metriken des Workload Analyzers in der lokalen NetApp Console-Bereitstellung".

Kapazitätswachstum eines Volumes in einer lokalen NetApp Console-Bereitstellung untersuchen

Der Workload Analyzer in der lokalen NetApp Console-Bereitstellung kann zur Untersuchung verwendet werden, warum ein Volume keinen Speicherplatz mehr hat.

Wenn ein Volume sich füllt oder Snapshot-Kopien mehr Speicherplatz belegen als erwartet, lassen sich die

Kapazitäts- und Snapshot-Trends im Zeitverlauf untersuchen. Der Abschnitt zur Kapazitätsanalyse zeigt, wie sich der physische und der verfügbare Speicherplatz verändern, schlüsselt die Einsparungen bei der Speichereffizienz auf und prognostiziert, wann das Volume eine Kapazitätsschwelle erreicht.

Wenn der Analysator über eine Warnung oder aus der Volumeninventur geöffnet wird, ist das Volumen bereits ausgewählt und der Fokus kann auf Kapazitätstrends und das Prognosefenster gelegt werden.

Schritte

1. Der Workload Analyzer kann mit einer der folgenden Methoden geöffnet werden:
   - Im Menü **Health** die Option **Workload Analyzer** auswählen, dann im Feld **Volume** nach dem Volume suchen und das gewünschte Volume zur Untersuchung auswählen.
   - Auf der Seite **Speicher > Flotten > Inventar** zu einem Volume navigieren, das analysiert werden soll, und im Aktionsmenü **Analysieren** auswählen.
   - Auf der Seite **Warnungen > Übersicht** eine Warnung für das Volumen auswählen, das untersucht werden soll, und dann in den Warnungsdetails **Analysieren** auswählen.
2. Den **Zeitraum** so einstellen, dass er den Zeitraum des Kapazitätswachstums abdeckt, dann **Analysieren** auswählen.
3. Zum Abschnitt **Kapazitätsanalyse** scrollen.
4. Im Dropdown-Menü **Ansicht** die Option **Kapazitätsansicht** auswählen.

   Das Diagramm zeigt die physische Kapazität als untere gestapelte Fläche und die verfügbare Kapazität als obere gestapelte Fläche. Zusammen ergeben sie die Gesamtvolumegröße, sodass ersichtlich ist, wie schnell der verfügbare Platz abnimmt.

5. Fahren Sie mit dem Mauszeiger über einen Punkt im Diagramm, um die Aufschlüsselung der Speichereffizienz einschließlich Einsparungen durch Deduplizierung, Komprimierung und Verdichtung sowie das Gesamtverhältnis der Speichereffizienz zu sehen.

   Ein sinkendes Effizienzverhältnis bei gleichzeitig steigender physischer Kapazität kann darauf hindeuten, dass neu geschriebene Daten nicht so gut dedupliziert oder komprimiert werden wie die vorhandenen Daten.

6. Zur Untersuchung des Snapshot-Verbrauchs im Dropdown-Menü **Ansicht** die Option **Snapshot View** auswählen.

   Das Diagramm zeigt die Snapshot-Reserve als horizontale Referenzlinie und die genutzte Snapshot-Kapazität als Fläche darunter. Beim Überfahren mit der Maus werden der genutzte Snapshot-Speicherplatz und dessen prozentualer Anteil an der Reserve, die Gesamtzahl der Snapshots sowie das Alter des ältesten Snapshots angezeigt.

   Wenn der Snapshot-Verbrauch die Reserve übersteigt, beginnen Snapshots, Speicherplatz aus dem Datenbereich des Volumes zu belegen, wodurch der für neue Schreibvorgänge verfügbare Speicherplatz reduziert wird.

7. Wenn das Volume Daten in die Cloud auslagert, kann im Dropdown-Menü **Ansicht** die Option **Cloud Tier View** ausgewählt werden, um zu vergleichen, wie viel Kapazität sich auf dem lokalen Performance Tier im Vergleich zum Cloud Capacity Tier befindet.
8. **Prognose anzeigen** aktivieren, um zu prognostizieren, wann das Volumen einen Warn- oder kritischen Kapazitätsschwellenwert erreicht.

   Die Kapazitätsprognose benötigt mindestens 10 Tage an historischen Daten. Wenn weniger als 30 Tage Kapazität verbleiben, bevor das Volume voll ist, identifiziert das Analysetool den Speicher als nahezu voll.

Die Prognose zeigt eine Insight-Meldung mit einer geschätzten Zeit bis zum Erreichen der Kapazitätsgrenze an.

Nachdem Sie fertig sind

Die beobachteten Kapazitätstrends können zur Entscheidungsfindung für die nächsten Schritte herangezogen werden:

- Wenn die verfügbare Kapazität fast voll ist, kann eine Erhöhung der Volume-Größe, das Aktivieren der automatischen Vergrößerung oder das Verschieben von Daten vom Volume in Betracht gezogen werden.
- Wenn die von Snapshots genutzte Kapazität die Reserve überschreitet, sollten die Snapshot-Richtlinie und die Aufbewahrungsfrist überprüft werden, um Speicherplatz zurückzugewinnen.
- Wenn das Speichereffizienzverhältnis sinkt, sollte geprüft werden, ob der Datentyp der Workload oder die Inline-Effizienzeinstellungen die Einsparungen verringern. Für detaillierte Beschreibungen von Kapazitäts-, Snapshot- und Effizienzmetriken "Informationen zu den Metriken des Workload Analyzers in der lokalen NetApp Console-Bereitstellung" verwenden.

Workload Analyzer-Metriken in der lokalen NetApp Console-Bereitstellung

In der lokalen Bereitstellung der NetApp Console zeigt der Workload Analyzer Metriken in sechs Abschnitten an. Jede Metrikbeschreibung erläutert, wie der Analyzer die Metrik im Diagramm darstellt und was sie über das Volumenverhalten aussagt.

QoS-Referenzlinien in Latenzdiagrammen

Wenn für das ausgewählte Volume eine QoS-Richtlinie verwendet wird, stehen im Metrik-Picker zwei zusätzliche Referenzzeilen zur Verfügung:

Referenzlinie	Beschreibung
Maximales QoS-Limit	Die maximale Latenzgrenze, die durch die QoS-Richtlinie definiert ist. Wenn die Latenzlinie sich dieser Grenze nähert oder sie berührt, drosselt ONTAP die Arbeitslast, und das QoS-Limit, nicht eine physische Ressource, ist die dominierende Ursache für die Latenz.
QoS-Limit (Min.)	Die durch die QoS-Richtlinie garantierte Mindestlatenz. Diese Zeile gibt die für die Arbeitslast durchgesetzte Antwortzeit-Untergrenze an. Wenn andere Arbeitslasten QoS-Mindestwerte verwenden, um ihren Durchsatz zu garantieren, kann ONTAP diese Arbeitslast drosseln, was dann zu einer höheren Latenz führt.

Diese horizontalen Linien werden beim Überfahren mit der Maus nicht in der Verzögerungszentrumsanalyse angezeigt. Sie dienen als Referenzschwellenwerte, nicht als Verursacher der Latenz.

Latenzaufschlüsselung nach I/O-Typ

Nutzen Sie die Aufschlüsselung der I/O-Typen im Abschnitt **Latenzanalyse**, nachdem im Dropdown-Menü „Ansicht“ die Option **Aufschlüsselung nach Verzögerungszentrum** ausgewählt wurde. Das Diagramm unterteilt die Gesamtlatenz in drei Kategorien, basierend auf der Richtung der I/O-Operation. Diese Metriken geben Aufschluss darüber, ob ein Leistungsproblem Lese-, Schreib- oder Metadatenoperationen betrifft.

Latenztyp	Beschreibung	Häufige Ursachen für erhöhte Werte
Leselatenz	Durchschnittliche Zeit für die Bearbeitung einer Leseanfrage eines Clients auf dem Volume, vom Eingang der Anfrage bis zur Rückgabe der Daten. Leseanfragen müssen den gesamten I/O-Pfad vom Netzwerkprotokoll durch den Datenverarbeitungs-Stack bis zu dem Aggregat durchlaufen, in dem sich die Daten befinden.	Aggregat- oder Festplattenkonflikte; Cache-Fehlzugriffe, die Lesevorgänge auf die physische Festplatte fördern; kalte Daten, die über eine Cloud-Kapazitätsebene mittels FabricPool abgerufen werden; knotenübergreifende Lesevorgänge, wenn sich die Daten auf einem anderen Knoten befinden als dem, der die Anfrage bearbeitet.
Schreiblatenz	Durchschnittliche Zeit bis zur Bestätigung einer Schreibanforderung eines Clients auf dem Volume. ONTAP bestätigt einen Schreibvorgang, sobald dieser im NVRAM Write-Log gespeichert wurde; die Daten werden anschließend in das Aggregat geschrieben.	Netzwerkkartenauslastung oder hohe Roundtrip-Latenz zwischen dem Client und dem Speicherknoten; synchroner SnapMirror, der auf die Bestätigung des Empfangs durch den Ziel-Cluster wartet, bevor der Schreibvorgang bestätigt werden kann; NVRAM-Druck bei hoher Schreiblast; CPU-Overhead durch Inline-Deduplizierung, Komprimierung oder Kompaktierung im Schreib-I/O-Pfad.
Andere Latenz	Durchschnittliche Zeit für alle Operationen auf dem Volume, die weder Lesen noch Schreiben erfordern, einschließlich Dateiöffnungen, Attributabfragen, Verzeichnisdurchläufe, Dateierstellungen und Sperren. Erhöhte andere Latenz kann die Reaktionsfähigkeit von Anwendungen beeinträchtigen, selbst wenn die Lese- und Schreiblatenz normal erscheint.	CPU-Belastung durch Inline-Effizienzoperationen, die mit der Metadatenverarbeitung konkurrieren; hohe Namespace-Aktivität durch Workloads, die eine große Anzahl von Dateierstellungen, -löschungen oder Verzeichnisscans erzeugen; QoS-Drosselung, die die Gesamt-IOPS einschränkt, sodass weniger IOPS für Metadatenoperationen verfügbar sind; Overhead bei der Volume-Aktivierung, wenn viele Volumes gleichzeitig aktiv sind.

Durchsatzkomponenten

Die Durchsatzkomponenten im Abschnitt **Throughput Analysis** werden nach Auswahl von **Breakdown (RWO)** im Dropdown-Menü „View“ angezeigt. Der Analyzer zeigt sowohl IOPS als auch MB/s gleichzeitig an.

Komponente	Beschreibung	Dargestellt als
Lese-IOPS	Lesevorgänge pro Sekunde.	Gestapelte Fläche im IOPS-Diagramm.
Schreib-IOPS	Schreibvorgänge pro Sekunde.	Gestapelte Fläche im IOPS-Diagramm.
Andere IOPS	Metadaten und andere Nicht-Daten-Operationen pro Sekunde.	Gestapelte Fläche im IOPS-Diagramm.
Lesen MB/s	Lesedurchsatz in Megabyte pro Sekunde.	Gestapelte Fläche im MB/s-Diagramm.
Schreib-MB/s	Schreibdurchsatz in Megabyte pro Sekunde.	Gestapelte Fläche im MB/s-Diagramm.

Komponente	Beschreibung	Dargestellt als
Cloud Durchsatz	Durchsatz in Megabyte pro Sekunde zwischen dem Volume und der Cloud-Kapazitäts-Tier. Diese Metrik erscheint nur für Workloads, die Kapazität über FabricPool in die Cloud tiern.	Gestapelte Fläche im MB/s-Diagramm.

Die Komponenten Lesen, Schreiben und Sonstige ergeben zusammen den Gesamt-IOPS- oder MB/s-Wert. Beim Überfahren des Diagramms mit dem Mauszeiger werden der Wert jeder Komponente, ihr prozentualer Anteil am Gesamtwert sowie die durchschnittliche I/O-Größe (MB/s ÷ IOPS) pro Kategorie angezeigt.

Kennzahlen zur Ressourcenauslastung

Im Abschnitt **Ressourcenauslastung** lassen sich die Kennzahlen zur Ressourcenauslastung einsehen. Der Analysator zeigt jede Ressource, die das Volume bedient, als eigene Zeile an. Ressourcen werden nicht gestapelt.

Knotenmetriken

Metrik	Beschreibung
Knotenauslastung	Gesamtauslastungsgrad des Knotens. Durch Überfahren mit der Maus werden die CPU-Auslastung, die Netzwerkauslastung und der verfügbare Spielraum für jeden Knoten angezeigt.
CPU-Auslastung	Prozentuale Auslastung der CPU-Kapazität des Knotens. Dieser Wert wird im Tooltip beim Überfahren mit der Maus angezeigt.
Netzwerkauslastung	Prozentsatz der ausgelasteten Knotennetzwerkkapazität. Dieser Wert wird im Tooltip beim Überfahren mit der Maus angezeigt.
Reserve	Die verbleibende Knotenkapazität steht für zusätzliche Arbeitslast zur Verfügung. Dieser Wert wird im Tooltip beim Überfahren mit der Maus angezeigt.

Aggregierte Kennzahlen

Metrik	Beschreibung
Aggregat-Auslastung	Prozentsatz der Festplattenauslastung für das Aggregat. Durch Überfahren mit dem Mauszeiger werden der Wert der Festplattenauslastung, die Anzahl der Volumes im Aggregat und der verfügbare Headroom angezeigt.
Festplatte belegt	Prozentsatz der Zeit, in der die Festplatten des Aggregats aktiv E/A-Operationen verarbeiten. Dieser Wert wird im Tooltip beim Überfahren mit der Maus angezeigt.
Anzahl der Volumes	Anzahl der aktuell auf dem Aggregat gehosteten Volumes. Dieser Wert wird im Tooltip beim Überfahren mit der Maus angezeigt.
Reserve	Verbleibende Aggregatkapazität, die für zusätzliche Arbeitslasten verfügbar ist. Dieser Wert wird im Tooltip angezeigt.

Wenn die Auslastungslinie eines Knotens oder eines Aggregats den Schwellenwert für hohe Auslastung überschreitet, der im Diagramm mit einer gestrichelten Referenzlinie gekennzeichnet ist, können andere Workloads auf dieser Ressource mit dem ausgewählten Volume um die I/O-Kapazität konkurrieren.

Kapazitätskennzahlen

Kapazitätsansicht

Im Abschnitt **Kapazitätsanalyse** lassen sich die Kennzahlen der Kapazitätsansicht überprüfen, nachdem im Dropdown-Menü „Ansicht“ die Option **Kapazitätsansicht** ausgewählt wurde.

Metrik	Beschreibung
Physische Kapazität	Der nach den Speicheroptimierungsmaßnahmen belegte Speicherplatz auf der Festplatte. Dies ist der unterste Bereich im Diagramm. Physisch + Verfügbar ergibt immer die Gesamtgröße des Volumens.
Verfügbare Kapazität	Der verbleibende freie Platz im Volumen. Dies ist der oberste gestapelte Bereich im Diagramm. Er verringert sich mit zunehmender Physical Capacity.
Speichereffizienzverhältnis	Gesamteffizienzverhältnis (logische Daten ÷ physische Daten). Im Tooltip beim Überfahren mit der Maus wird dieser Wert angezeigt. Er spiegelt die kombinierten Einsparungen durch Deduplizierung, Komprimierung und Verdichtung wider.
Einsparungen durch Deduplizierung	Speicherplatz wird durch das Entfernen doppelter Datenblöcke eingespart. Dieser Wert wird im Tooltip beim Überfahren mit der Maus angezeigt.
Einsparungen durch Kompression	Durch die Inline-Komprimierung von Daten wird Speicherplatz eingespart. Der Tooltip beim Überfahren mit der Maus zeigt diesen Wert an.
Einsparungen bei der Verdichtung	Platzersparnis durch das Zusammenfassen mehrerer kleiner Blöcke zu einem einzigen physischen Block. Der Tooltip beim Überfahren mit der Maus zeigt diesen Wert an.

Momentaufnahmeansicht

Die Snapshot-Ansicht eignet sich, um Snapshot-spezifische Metriken zu überprüfen.

Metrik	Beschreibung	Dargestellt als
Verfügbare Momentaufnahme	Vorab zugewiesener Speicherplatz, der als Prozentsatz der Volume-Größe konfiguriert ist und für Snapshots reserviert wird.	Horizontale Bezugslinie.
Verwendeter Snapshot	Tatsächlich von Snapshot-Kopien belegter Speicherplatz.	Flächendiagramm unterhalb der Reservelinie.

Bewegen Sie den Mauszeiger über das Diagramm, um die Größe der Snapshot-Reserve, den belegten Snapshot-Speicherplatz und dessen prozentualen Anteil an der Reserve, die Gesamtzahl der Snapshots sowie das Alter des ältesten Snapshots zu sehen. Wenn der Snapshot-Verbrauch die Reserve überschreitet, belegen Snapshots Speicherplatz im Datenbereich des Volumes.

Prognoseverhalten

Verwenden Sie die Option „Prognose anzeigen“ in einem beliebigen Analyseabschnitt, wenn zukünftige Werte über den aktuellen Zeitpunkt hinaus basierend auf dem beobachteten Trend projiziert werden sollen. Die folgenden Verhaltensweisen gelten für alle Abschnitte:

Aspekt	Verhalten
Projektionsfenster	Projektionen erfolgen basierend auf dem ausgewählten Zeitraum. Bei einer 2-Stunden-Ansicht beträgt das Projektionsfenster etwa 1 Stunde. Bei einer 7-Tage-Ansicht erstreckt sich das Projektionsfenster über mehrere Tage.
Visueller Stil	Der Analysator stellt Prognosewerte als gestrichelte Linie dar. Eine vertikale Trennlinie markiert die Grenze zwischen Ist-Daten und prognostizierten Werten.
Schwellenwertwarnungen	Der Analysator zeigt eine Hinweismeldung an, wenn die Prognose darauf hindeutet, dass das Volumen einen Warn- oder kritischen Schwellenwert überschreiten wird, zusammen mit einer geschätzten Zeit bis zum Überschreiten.
Trendbasis	Die Prognose verwendet die Änderungsrate des jüngsten Abschnitts des ausgewählten Zeitraums. Hohe Volatilität in den aktuellen Daten verringert das Vertrauen in die Prognose.
Mindestdaten erforderlich	Für die Kapazitätsprognose werden mindestens 10 Tage an historischen Daten benötigt. Wenn weniger als 30 Tage Kapazität verbleiben, bevor das Volume voll ist, identifiziert das Analysesystem den Speicher als nahezu voll.

Verwandte Informationen

- "Informationen zum Workload Analyzer für die lokale Bereitstellung der NetApp Console"
- "Hohe Latenz auf einem Volumen untersuchen"
- "Untersuchung hoher Anforderungen an den Durchsatz eines Volumes"
- "Kapazitätswachstum eines Volumens untersuchen"

Lokale NetApp Console-Bereitstellung verwalten und überwachen

Informationen zur Administration und Überwachung in der lokalen NetApp Console-Bereitstellung

Nach der Bereitstellung der NetApp Console lokalen Bereitstellung können die Verwaltungs- und Überwachungstools genutzt werden, um Aktivitäten zu überprüfen, die VM zu warten und den Mitgliederzugriff zu verwalten.

Prüfungsaktivität

Benutzer- und API-Aktivitäten können überprüft, der Status von Console-Vorgängen nachverfolgt, Audit-Protokolle heruntergeladen und Protokolle zu externen Tools exportiert werden, wenn eine längere Aufbewahrung oder zusätzliche Analysen erforderlich sind.

- "Audit NetApp Console lokale Bereitstellungsaktivität"
- "Benachrichtigungszustellungskanäle in der lokalen NetApp Console-Bereitstellung einrichten"

Licenses and subscriptions

Die Informationen zu Licenses and subscriptions geben Aufschluss über Serviceberechtigungen und den Abonnementstatus für Ihre NetApp Console-Umgebung.

"Informationen zu Licenses and subscriptions".

Wartung und Fehlerbehebung der lokalen Console Bereitstellungs-VM

Die VM, die die lokale Console-Bereitstellung hostet, wird gewartet, Netzwerk- und Systemeinstellungen werden überprüft, auf Diagnosetools wird zugegriffen und Probleme werden behoben, wenn der Dienst oder der Agent sich nicht wie erwartet verhält.

"Pflegen Sie Ihren vCenter oder ESXi Host für die lokale Console-Bereitstellung".

Benutzer und Zugriff verwalten

Die Zugriffsrechte der Mitglieder in der gesamten Organisation können überprüft, auf Flottenebene angepasst und Sicherheitseinstellungen wie MFA-Wiederherstellung und Anmeldeinformationen für Dienstkonten verwaltet werden.

- "Mitgliederzugriff in der NetApp Console verwalten"
- "Flottenzugriffszuweisungen in der lokalen NetApp Console-Bereitstellung anzeigen oder ändern"
- "Mitgliedersicherheit in der lokalen NetApp Console-Bereitstellung verwalten"

Audit NetApp Console lokale Bereitstellungsaktivität

Auf der Seite „Audit“ lassen sich Benutzeraktivitäten, die sowohl über die Benutzeroberfläche als auch über die API initiiert wurden, prüfen, und der Status von Vorgängen in der lokalen NetApp Console-Bereitstellung sowie der Benutzer, der sie initiiert hat, kann überwacht werden.

Erforderliche Rollen

Super Admin, Organization Admin, Ordner- und Flotten-Admin, Operations Support Analyst, Super Viewer, Organization Viewer oder Ordner- und Flotten-Viewer. "Informationen zu Zugriffsrollen".

Sie können die Revisionsaktivitäten in der lokalen NetApp Console-Bereitstellung anzeigen, eine CSV-Datei des Revisionsprotokolls herunterladen oder das Revisionsprotokoll so konfigurieren, dass es mithilfe eines Webhooks an Ihren eigenen Syslog-Server gesendet wird.

Benutzeraktivitäten auf der Seite „Audit“ prüfen

Auf der Seite „Revisionsprotokoll“ lässt sich erkennen, wer eine Aktion durchgeführt hat oder welchen Status sie hat.

Die Seite „Audit“ zeigt die Aktionen an, die Benutzer in Ihrer Organisation durchgeführt haben. Beispielsweise lässt sich nachvollziehen, wer ein Mitglied zu einer Organisation hinzugefügt hat oder ob eine Flotte erfolgreich gelöscht wurde, ebenso wie weitere Speicherverwaltungsaktionen, die Benutzer in Ihrer Organisation durchgeführt haben.

Die Revisionsprotokolle zeigen Aktivitäten für die folgenden Dienste:

- Mandantenfähigkeit: Aktionen im Zusammenhang mit der Verwaltung Ihrer Organisation, wie das Hinzufügen von Benutzern, das Erstellen von Flotten und das Zuordnen von Ressourcen.
- Speicherverwaltung: Aktionen im Zusammenhang mit der Verwaltung Ihrer Speicherressourcen.
- Föderation: Maßnahmen im Zusammenhang mit der Verwaltung von Föderationen, wie das Erstellen von Föderationen und das Hinzufügen oder Entfernen von föderierten Organisationen.

Schritte

1. **Verwaltung > Revisionsprotokoll** auswählen.
2. Mit den Filtern oberhalb der Tabelle lässt sich steuern, welche Aktionen in der Tabelle angezeigt werden.

   Beispielsweise kann der Filter **Service** verwendet werden, um Aktionen anzuzeigen, die sich auf einen bestimmten Dienst beziehen, oder der Filter **User** kann verwendet werden, um Aktionen anzuzeigen, die sich auf ein bestimmtes Benutzerkonto beziehen.

Revisionsprotokolle nach Aktionen im Bereich Identitäts- und Zugriffsmanagement filtern

Um nur Aktionen im Zusammenhang mit der Verwaltung Ihrer Organisation wie das Hinzufügen von Mitgliedern, das Erstellen von Flotten oder das Löschen von Ressourcen anzuzeigen, das Revisionsprotokoll nach dem Mandantendienst filtern.

Schritte

1. **Verwaltung > Revisionsprotokoll** auswählen.
2. Verwenden Sie die Filter, um die Ergebnisse einzugrenzen. **Service** auswählen und dann **Tenancy** auswählen.
3. Mit den anderen Filtern lassen sich die Ergebnisse weiter verfeinern.

   Beispielsweise kann der Filter **User** verwendet werden, um IAM-Aktionen anzuzeigen, die von einem bestimmten Benutzerkonto ausgeführt wurden.

Audit-Protokolle von der Audit-Seite herunterladen

Sie können die Revisionsprotokolle von der Seite „Revisionsprotokoll“ als CSV-Datei herunterladen. Dadurch wird eine Aufzeichnung der Aktionen ermöglicht, die Benutzer in Ihrer Organisation ausführen. Die heruntergeladene CSV-Datei enthält alle Revisionsprotokollspalten, unabhängig von den Filtern oder angezeigten Spalten auf der Seite „Revisionsprotokoll“.

Schritte

1. Auf der Seite **Audit** das Download-Symbol in der oberen rechten Ecke der Tabelle auswählen.

NetApp Console warten

Pflegen Sie Ihren vCenter oder ESXi-Host für die lokale Bereitstellung der NetApp Console

In der lokalen NetApp Console-Bereitstellung können nach der Bereitstellung Änderungen an Ihrem bestehenden VCenter- oder ESXi-Host vorgenommen werden. Beispielsweise ist es möglich, die CPU oder den Arbeitsspeicher der VM-Instanz zu erhöhen, die die Console lokale Bereitstellung hostet.

Diese Wartungsaufgaben lassen sich über die VM-Webkonsole ausführen:

- Festplattengröße vergrößern
- Die lokale NetApp Console-Bereitstellung neu starten
- Statische Routen aktualisieren
- Suchdomänen aktualisieren

Einschränkungen

Über die Wartungskonsole können Sie lediglich Informationen zur IP-Adresse, zum DNS und zu den Gateways anzeigen (nicht aktualisieren).

Zugriff auf die VM-Wartungskonsole

Über den vSphere Client ist ein Zugriff auf die Wartungskonsole möglich.

Schritte

1. Öffnen Sie den vSphere Client und melden Sie sich bei Ihrem vCenter an.
2. Wählen Sie die VM-Instanz aus, die die lokale NetApp Console-Bereitstellung hostet.
3. **Webkonsole starten** auswählen.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Passwort an, die Sie bei der Erstellung der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Passwort ist dasjenige, das Sie bei der Erstellung der VM-Instanz angegeben haben.

Das Wartungsbenutzerpasswort ändern

Sie können das Passwort für den `maint` Benutzer ändern.

Schritte

1. Öffnen Sie den vSphere Client und melden Sie sich bei Ihrem vCenter an.
2. Wählen Sie die VM-Instanz aus, die die lokale NetApp Console-Bereitstellung hostet.
3. **Webkonsole starten** auswählen.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Passwort an, die Sie bei der Erstellung der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Passwort ist dasjenige, das Sie bei der Erstellung der VM-Instanz angegeben haben.
5. Geben Sie `1` ein, um das `System Configuration` Menü anzuzeigen.
6. Geben Sie `1` ein, um das Wartungsbenutzerpasswort zu ändern, und folgen Sie den Anweisungen auf dem Bildschirm.

CPU oder RAM der VM-Instanz erhöhen

Sie können die CPU oder den RAM der VM-Instanz erhöhen, die die lokale NetApp Console-Bereitstellung hostet.

Die Einstellungen der VM-Instanz im vCenter oder ESXi-Host werden bearbeitet, anschließend werden die Änderungen über die Wartungskonsole angewendet.

Schritte im vSphere Client

1. Öffnen Sie den vSphere Client und melden Sie sich bei Ihrem vCenter an.
2. Wählen Sie die VM-Instanz aus, die die lokale NetApp Console-Bereitstellung hostet.
3. Klicken Sie mit der rechten Maustaste auf die VM-Instanz und wählen Sie **Einstellungen bearbeiten**.
4. Erhöhen Sie den für /opt oder die /var-Partition verwendeten Festplattenspeicher.
   a. **Festplatte 2** auswählen, um den für /opt verwendeten Festplattenspeicher zu erhöhen.
   b. **Festplatte 3** auswählen, um den für /var verwendeten Festplattenspeicher zu erhöhen.
5. Speichern Sie Ihre Änderungen.

Schritte in der Wartungskonsole

1. Öffnen Sie den vSphere Client und melden Sie sich bei Ihrem vCenter an.
2. Wählen Sie die VM-Instanz aus, die die lokale NetApp Console-Bereitstellung hostet.
3. **Webkonsole starten** auswählen.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Passwort an, die Sie bei der Erstellung der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Passwort ist dasjenige, das Sie bei der Erstellung der VM-Instanz angegeben haben.
5. Menü `1 to view the `System Configuration` aufrufen.
6. Geben Sie `2` ein und folgen Sie den Anweisungen auf dem Bildschirm. Die Konsole sucht nach neuen Einstellungen und vergrößert die Größe der Partitionen.

Netzwerkeinstellungen für die lokale Console-Bereitstellungs-VM anzeigen

Die Netzwerkeinstellungen der Console lokalen Bereitstellungs-VM im VSphere-Client können angezeigt werden, um Netzwerkprobleme zu bestätigen oder zu beheben. Es können lediglich die folgenden Netzwerkeinstellungen angezeigt werden (kein Update möglich): IP-Adresse und DNS-Details.

Schritte

1. Öffnen Sie den vSphere Client und melden Sie sich bei Ihrem vCenter an.
2. Wählen Sie die VM-Instanz aus, die die lokale NetApp Console-Bereitstellung hostet.
3. **Webkonsole starten** auswählen.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Passwort an, die Sie bei der Erstellung der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Passwort ist dasjenige, das Sie bei der Erstellung der VM-Instanz angegeben haben.
5. Geben Sie `2` ein, um das `Network Configuration` Menü anzuzeigen.
6. Geben Sie eine Zahl zwischen 1 und 6 ein, um die entsprechenden Netzwerkeinstellungen anzuzeigen.

Die statischen Routen für die lokale NetApp Console-Bereitstellungs-VM aktualisieren

Statische Routen für die lokale NetApp Console-Bereitstellungs-VM können nach Bedarf hinzugefügt, aktualisiert oder entfernt werden.

Schritte

1. Öffnen Sie den vSphere Client und melden Sie sich bei Ihrem vCenter an.
2. Wählen Sie die VM-Instanz aus, die die lokale NetApp Console-Bereitstellung hostet.
3. **Webkonsole starten** auswählen.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Passwort an, die Sie bei der Erstellung der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Passwort ist dasjenige, das Sie bei der Erstellung der VM-Instanz angegeben haben.
5. Geben Sie `2` ein, um das `Network Configuration` Menü anzuzeigen.
6. Geben Sie `7` ein, um statische Routen zu aktualisieren und den Anweisungen auf dem Bildschirm zu folgen.
7. Drücken Sie die Eingabetaste.
8. Optional sind weitere Änderungen möglich.

9. Geben Sie `9` ein, um Ihre Änderungen zu übernehmen.

Domänensucheinstellungen für die lokale NetApp Console-Bereitstellungs-VM aktualisieren

Sie können die Suchdomäneneinstellungen für die lokale NetApp Console VM-Instanz aktualisieren.

Schritte

1. Öffnen Sie den vSphere Client und melden Sie sich bei Ihrem vCenter an.
2. Wählen Sie die VM-Instanz aus, die die lokale NetApp Console-Bereitstellung hostet.
3. **Webkonsole starten** auswählen.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Passwort an, die Sie bei der Erstellung der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Passwort ist dasjenige, das Sie bei der Erstellung der VM-Instanz angegeben haben.
5. Geben Sie `2` ein, um das `Network Configuration` Menü anzuzeigen.
6. Geben Sie `8` ein, um die Einstellungen für die Domänensuche zu aktualisieren, und folgen Sie den Anweisungen auf dem Bildschirm.
7. Drücken Sie die Eingabetaste.
8. Optional sind weitere Änderungen möglich.
9. Geben Sie `9` ein, um Ihre Änderungen zu übernehmen.

Zugriff auf die lokalen Bereitstellungsdiagnosetools der Konsole

Diagnosetools stehen zur Verfügung, um Probleme mit der lokalen Console-Bereitstellung zu beheben. NetApp Support kann darum bitten, dies im Rahmen der Fehlerbehebung zu tun.

Schritte

1. Öffnen Sie den vSphere Client und melden Sie sich bei Ihrem vCenter an.
2. Wählen Sie die VM-Instanz aus, die die lokale NetApp Console-Bereitstellung hostet.
3. **Webkonsole starten** auswählen.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Passwort an, die Sie bei der Erstellung der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Passwort ist dasjenige, das Sie bei der Erstellung der VM-Instanz angegeben haben.
5. Geben Sie `3` ein, um das Menü „Support und Diagnose“ anzuzeigen.
6. Geben Sie `1` ein, um auf die Diagnosetools zuzugreifen und den Anweisungen auf dem Bildschirm zu folgen.

Remote-Zugriff auf die lokalen Bereitstellungsdiagnosetools der Konsole

Mit einem Tool wie PuTTY ist der Remote-Zugriff auf Diagnosetools möglich. Der SSH-Zugriff auf die lokale VM der Console-Bereitstellung wird durch die Vergabe eines Einmalpassworts ermöglicht.

SSH-Zugriff ermöglicht erweiterte Terminalfunktionen wie Kopieren und Einfügen.

Schritte

1. Öffnen Sie den vSphere Client und melden Sie sich bei Ihrem vCenter an.
2. Wählen Sie die VM-Instanz aus, die die lokale NetApp Console-Bereitstellung hostet.

3. **Webkonsole starten** auswählen.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Passwort an, die Sie bei der Erstellung der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Passwort ist dasjenige, das Sie bei der Erstellung der VM-Instanz angegeben haben.
5. Geben Sie `3` ein, um das `Support and Diagnostics` Menü anzuzeigen.
6. Geben Sie `2` ein, um auf die Diagnosetools zuzugreifen, und folgen Sie den Anweisungen auf dem Bildschirm, um ein Einmalpasswort zu konfigurieren, das nach 24 Stunden abläuft.
7. Verwenden Sie ein SSH-Tool wie Putty, um mit dem Benutzernamen `diag` und dem von Ihnen konfigurierten Einmalpasswort eine Verbindung zur lokalen VM-Bereitstellung der Konsole herzustellen.

Benutzer und Zugriff verwalten

Mitgliederzugriff in der lokalen NetApp Console-Bereitstellung verwalten

In der lokalen NetApp Console-Bereitstellung können die Rollen eines Benutzers über mehrere Ordner oder Flotten hinweg überprüft oder geändert werden, etwa um alles zu sehen, worauf ein Storage-Ingenieur Zugriff hat, eine neue Rolle in einer anderen Region hinzuzufügen oder den Zugriff dieses Benutzers zu entfernen, wenn sich die Zuständigkeiten ändern.

Erforderliche Zugriffsrollen

Superadministrator, Organisationsadministrator oder Ordner- bzw. Flottenadministrator (für die von ihnen verwalteten Ordner und Flotten). "Informationen zu Zugriffsrollen".

Sie können die Zugriffsrechte je nach Bedarf auf zwei Arten einsehen und verwalten. Wenn die Rollen eines bestimmten Benutzers in der gesamten Flotte Ihrer Organisation angezeigt werden sollen, ist die Seite **Members** zu verwenden.

Wenn Sie überprüfen möchten, wer Zugriff auf eine bestimmte Flotte hat, sollten stattdessen die dieser Flotte zugewiesenen Mitglieder überprüft werden. "Flottenzugriffszuweisungen verwalten".

Um ein neues Mitglied, ein Servicekonto oder einen Verzeichnisbenutzer hinzuzufügen und die erste Rolle zuzuweisen, sollte stattdessen die Onboarding-Aufgabe verwendet werden. "Mitglieder hinzufügen und Rollen zuweisen".

Informationen darüber, wie der Zugriff in der NetApp Console gewährt wird

NetApp Console verwendet rollenbasierte Zugriffssteuerung (RBAC) zur Verwaltung von Mitgliedsberechtigungen. Vordefinierte Rollen können auf Organisations-, Ordner- oder Flottenebene zugewiesen werden, abhängig vom benötigten Zugriffsumfang eines Mitglieds.

Verwendung der Rollenvererbung

Eine Rolle, die Sie auf Organisations- oder Ordnerebene zuweisen, wird von den darunterliegenden Unterbereichen geerbt, daher sollte eine geerbte Zuweisung in dem übergeordneten Bereich geändert werden, in dem sie ursprünglich vergeben wurde.

"Informationen zur Rollenvererbung in der lokalen Bereitstellung der NetApp Console".

Zugewiesene Rollen eines Mitglieds anzeigen

Bestätigen Sie genau, welche Rollen ein Mitglied innehat und auf welcher Ebene, bevor eine Änderung vorgenommen wird. Beispielsweise kann überprüft werden, ob ein Teammitglied bereits die Storage admin Rolle auf der `Production-EU-West` Flotte hat.

Wenn Sie die Rolle „Ordner- oder Flottenadministrator“ besitzen, werden auf der Seite alle Mitglieder in der Organisation angezeigt. Es können jedoch nur die Berechtigungen für die Ordner und Flotten angezeigt und verwaltet werden, die Sie administrieren. "Informationen zu Ordner- oder Flottenadministratoraktionen in der lokalen Bereitstellung der NetApp Console".

1. Auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle navigieren, ••• auswählen und anschließend **Details anzeigen** wählen.
2. In der Tabelle die entsprechende Zeile für die Organisation, den Ordner oder die Flotte erweitern, in der die zugewiesene Rolle des Mitglieds angezeigt werden soll, und in der Spalte **Rolle Anzeigen** auswählen.

Mitgliederzugriff zuweisen oder ändern

Sie können die Zugriffsrechte eines Mitglieds anpassen, sobald sich dessen Verantwortlichkeiten ändern. Wenn beispielsweise ein Teammitglied die Backup und Recovery Administratorrolle für die Flotte einer zweiten Region übernimmt, kann diese Rolle für die betreffende Region hinzugefügt werden, ohne die bestehenden Speicherrollen zu verändern.

Wenn ein neues Mitglied hinzugefügt und ihm seine erste Rolle zugewiesen werden soll, siehe "Mitglieder hinzufügen und Rollen zuweisen".

Einer bestehenden Mitgliedsperson eine Zugriffsrolle hinzufügen

Einem Mitglied kann auf Organisations-, Ordner- oder Flottenebene eine zusätzliche Rolle zugewiesen werden, wenn sich dessen Verantwortlichkeiten erweitern. Beispielsweise erhält ein Storage-Administrator die Backup und Recovery Admin-Rolle auf Organisationsebene, sodass Backup und Recovery Aufgaben über alle Flotten hinweg verwaltet werden können, ohne dass die bestehenden Speicherberechtigungen verloren gehen.

Sie können einem Mitglied eine Zugriffsrolle für Ihre Organisation, Ihren Ordner oder Ihre Flotte zuweisen.

Mitglieder können innerhalb derselben Flotte und in verschiedenen Flotten mehrere Rollen innehaben. Beispielsweise können kleinere Organisationen einem Benutzer alle verfügbaren Zugriffsrollen zuweisen, während größere Organisationen Benutzern spezialisiertere Aufgaben zuweisen. Alternativ kann einem Benutzer die Ransomware resilience Admin-Rolle auf Organisationsebene zugewiesen werden. In diesem Beispiel wäre der Benutzer in der Lage, Ransomware resilience Aufgaben für alle Flotten innerhalb Ihrer Organisation auszuführen.

Ihre Zugriffsrollenstrategie sollte mit der Art und Weise übereinstimmen, wie Sie Ihre NetApp Ressourcen organisiert haben.

Schritte

1. **Verwaltung > Identität und Zugriff** auswählen.
2. **Mitglieder** auswählen.
3. Wählen Sie eine der Mitglieds-Registerkarten aus: **Benutzer**, **Verzeichnisbenutzer** oder **Dienstkonten**.
4. Wählen Sie das Aktionen-Menü ••• neben dem Mitglied, dem Sie eine Rolle zuweisen möchten, und wählen Sie **Rolle hinzufügen** aus.
5. Zum Hinzufügen einer Rolle sind die Schritte im Dialogfeld auszuführen:

- **Organisation, Ordner oder Flotte auswählen**: Die Ebene der Ressourcenhierarchie auswählen, für die das Mitglied Berechtigungen erhalten soll.

  Wenn die Organisation oder ein Ordner ausgewählt wird, hat das Mitglied Berechtigungen für alles, was sich innerhalb der Organisation oder des Ordners befindet.

- **Kategorie auswählen**: Eine Rollenkategorie auswählen. "Informationen zu Zugriffsrollen".
- Wählen Sie eine **Rolle**: Es ist eine Rolle auszuwählen, die dem Mitglied Berechtigungen für die Ressourcen gewährt, die mit der ausgewählten Organisation, dem Ordner oder der Flotte verknüpft sind.
- **Rolle hinzufügen**: Wenn Sie Zugriff auf zusätzliche Ordner oder Flotten innerhalb Ihrer Organisation gewähren möchten, wählen Sie **Rolle hinzufügen**, geben Sie einen anderen Ordner, eine andere Flotte oder eine andere Rollenkategorie an und wählen Sie dann eine Rollenkategorie und eine entsprechende Rolle.

6. **Neue Rollen hinzufügen** auswählen.

Die einem Mitglied zugewiesene Rolle ändern

Ersetzen Sie die bestehende Rolle eines Mitglieds durch eine andere, wenn sich dessen Verantwortlichkeiten ändern. Zum Beispiel, wenn ein Storage Viewer in der `Production-US-East` Flotte stattdessen die Storage Admin-Rolle benötigt.

Jeder Benutzer muss mindestens eine Rolle haben. Es können nicht alle Rollen von einem Benutzer entfernt werden. Wenn alle Rollen entfernt werden müssen, ist der Benutzer aus Ihrer Organisation zu löschen.

Schritte

1. **Verwaltung > Identität und Zugriff** auswählen.
2. **Mitglieder** auswählen.
3. Wählen Sie eine der Mitglieds-Registerkarten aus: **Benutzer**, **Verzeichnisbenutzer** oder **Dienstkonten**.
4. Auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle navigieren, ••• auswählen und anschließend **Details anzeigen** wählen.
5. In der Tabelle die entsprechende Zeile für die Organisation, den Ordner oder die Flotte erweitern, in der die zugewiesene Rolle des Mitglieds geändert werden soll, und in der Spalte **Rolle Anzeigen** auswählen, um die diesem Mitglied zugewiesenen Rollen anzuzeigen.
6. Sie können eine bestehende Rolle für ein Mitglied ändern oder eine Rolle entfernen.
   a. Um die Rolle eines Mitglieds zu ändern, **Ändern** neben der Rolle auswählen, die geändert werden soll. Eine Rolle kann nur in eine Rolle innerhalb derselben Rollenkategorie geändert werden. Beispielsweise ist ein Wechsel von einer Datendienstrolle zu einer anderen möglich. Die Änderung bestätigen.
   b. Um einem Mitglied die Rolle zu entziehen, 🗑 neben der entsprechenden Rolle auswählen, um dem Mitglied die jeweilige Rolle zu entziehen. Es erfolgt eine Aufforderung, die Entfernung zu bestätigen.

Ein Mitglied aus Ihrer Organisation entfernen

Ein Mitglied wird entfernt, wenn es die Organisation verlässt oder seine Rolle so ändert, dass kein Zugriff auf die Console mehr erforderlich ist. Zum Beispiel, wenn der Auftrag eines externen Dienstleisters endet oder ein Mitarbeiter in ein Team außerhalb Ihrer Console-Organisation wechselt.

Verzeichnisbenutzer

Wenn Sie einen Benutzer aus Ihrem Verzeichnis entfernen, kann sich dieser Benutzer nicht mehr authentifizieren. Der Benutzer sollte außerdem aus Ihrer Console Organisation entfernt werden, um die Mitgliederliste korrekt zu halten und alle Rollen zu entfernen, die ihm bei der lokalen Console Bereitstellung zugewiesen wurden.

Schritte

1. **Verwaltung > Identität und Zugriff** auswählen.
2. **Mitglieder** auswählen.
3. Wählen Sie eine der Mitglieds-Registerkarten aus: **Benutzer**, **Verzeichnisbenutzer** oder **Dienstkonten**.
4. Auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle navigieren, ••• auswählen und anschließend **Benutzer löschen** wählen.
5. Bestätigen Sie, dass das Mitglied aus Ihrer Organisation entfernt werden soll.

Flottenzugriffszuweisungen in der lokalen NetApp Console-Bereitstellung anzeigen oder ändern

Auditieren oder ändern Sie die Zugriffszuweisungen von Mitgliedern für Ordner und Storage Fleets in der lokalen NetApp Console-Bereitstellung. Ordner- und Fleet-Administratoren arbeiten typischerweise mit dieser Ansicht, da sie nur die Bereiche anzeigt, die sie verwalten.

Erforderliche Zugriffsrollen

Superadministrator, Organisationsadministrator oder Ordner- oder Flottenadministrator. "Informationen zu Zugriffsrollen".

Alternativ ist es möglich, alle Rollen eines bestimmten Mitglieds über mehrere Ordner oder Flotten hinweg zu verwalten. "Mitgliederzugriff verwalten".

Funktionsweise des Ordner- und Flottenzugriffs

Die lokale Bereitstellung über die Console verwendet rollenbasierte Zugriffssteuerung (RBAC). Eine Rolle, die auf Ordnerebene zugewiesen wird, gilt für alle Flotten und Unterordner innerhalb dieses Ordners; eine Rolle, die auf Flottenebene zugewiesen wird, gilt nur für die Ressourcen dieser Flotte. "Informationen zur Rollenvererbung in der lokalen Bereitstellung der NetApp Console".

Eine Rolle kann auf Flottenebene nicht geändert werden, wenn ein Mitglied sie von einem Ordner oder von der Organisation erbt. Um geerbten Zugriff zu ändern, muss die Rolle auf der höheren Ebene geändert werden.

Anzeigen der Mitglieder, die einem Ordner oder einer Flotte zugewiesen sind

Es kann genau überprüft werden, wer einen bestimmten Ordner oder eine bestimmte Flotte verwalten kann. Beispielsweise lässt sich vor der Zuordnung eines neuen Produktions-ONTAP Clusters zur `Production-US-East` Flotte auf der Registerkarte „Zugriff“ der Flotte nachvollziehen, wer Zugriff hat.

Schritte

1. **Administration** > **Identität und Zugriff** auswählen.
2. **Organisation** auswählen.

3. Auf der Seite „Organisation“ zu einem Ordner oder einer Flotte in der Tabelle navigieren, ••• und dann **Ordner bearbeiten** oder **Flotte bearbeiten** auswählen.
4. **Zugriff** zeigt die Mitglieder an, die Zugriff auf den Ordner oder die Flotte haben.

Mitgliederzugriff über einen Ordner oder eine Flotte ändern

Passen Sie die Rollen von Mitgliedern, die bereits zu Ihrer Organisation gehören, an, beschränkt auf einen einzelnen Ordner oder eine einzelne Flotte. Wenn beispielsweise ein Teammitglied von einer Entwicklungsflotte in eine Produktionsflotte wechselt, kann es in der Produktionsflotte vom Storage viewer zum Storage admin befördert werden, ohne dass der Zugriff an anderen Stellen beeinflusst wird.

Um ein neues Mitglied hinzuzufügen und ihm seine erste Rolle zuzuweisen, sollte stattdessen die Onboarding-Aufgabe verwendet werden. "Mitglieder hinzufügen und Rollen zuweisen".

Schritte

1. Auf der Seite „Organisation“ zu einem Ordner oder einer Flotte in der Tabelle navigieren, ••• und dann **Ordner bearbeiten** oder **Flotte bearbeiten** auswählen.
2. **Zugriff** auswählen, um die Liste der Mitglieder anzuzeigen, die Zugriff haben.
3. Mitgliederzugriff ändern:
   - **Mitgliedsrolle ändern**: Für jedes Mitglied mit einer anderen Rolle als Organization admin die bestehende Rolle auswählen und eine neue Rolle festlegen. Die Änderung gilt nur für diesen Bereich; Rollen, die von einem höheren Bereich geerbt wurden, werden hier nicht angezeigt.
   - **Mitgliedszugriff in diesem Bereich entfernen**: Für ein Mitglied, dessen Rolle direkt in diesem Ordner oder dieser Flotte definiert ist, wird durch das Entfernen der Rolle der Zugriff in diesem Bereich widerrufen. Dadurch wird das Mitglied nicht aus Ihrer Organisation entfernt und Rollen in anderen Bereichen bleiben unberührt.

     "Ein Mitglied aus Ihrer Organisation entfernen".
4. **Anwenden** auswählen.

Mitgliedersicherheit in der lokalen NetApp Console-Bereitstellung verwalten

Der Benutzerzugriff auf die lokale NetApp Console-Bereitstellungsorganisation wird durch die Verwaltung der Sicherheitseinstellungen der Mitglieder geschützt. Lokale Benutzer können dazu angeleitet werden, ihre eigenen Passwörter zu ändern, die Multi-Faktor-Authentifizierung (MFA) lokaler Benutzer zu verwalten und die Anmeldeinformationen für Dienstkonten neu zu erstellen.

Erforderliche Zugriffsrollen

Superadministrator, Organisationsadministrator oder Ordner- oder Flottenadministrator. "Informationen zu Zugriffsrollen".

Benutzerpasswörter zurücksetzen (nur lokale Benutzer)

Administratoren können lokale Benutzerpasswörter nicht direkt zurücksetzen.

Lokale Benutzer werden darauf hingewiesen, ihre Passwörter auf der Anmeldeseite der lokalen NetApp Console-Bereitstellung zurückzusetzen, indem sie **Passwort vergessen?** auswählen.

Diese Option steht Verzeichnisbenutzern nicht zur Verfügung.

Multi-Faktor-Authentifizierung (MFA) eines lokalen Benutzers verwalten

Wenn ein lokaler Benutzer den Zugriff auf sein MFA-Gerät verliert, kann entweder die MFA-Konfiguration entfernt oder deaktiviert werden.

Multi-Faktor-Authentifizierung ist nur für lokale Benutzer verfügbar. Verzeichnisbenutzer können MFA nicht über die lokale Bereitstellung in der NetApp Console aktivieren.

Diese Richtlinien helfen bei der Auswahl der richtigen Maßnahme:

- **Deaktivieren** auswählen, wenn der Benutzer vorübergehend keinen Zugriff auf sein MFA-Gerät hat. Durch Deaktivieren von MFA ist eine Anmeldung ohne MFA für acht Stunden möglich, anschließend wird MFA automatisch wieder aktiviert.
- **Entfernen** auswählen, wenn der Benutzer die Multi-Faktor-Authentifizierung (MFA) vollständig zurücksetzen muss. Nach dem Entfernen der MFA meldet sich der Benutzer ohne MFA an, bis er die MFA erneut konfiguriert.

Verfügt ein Benutzer über einen gespeicherten Wiederherstellungscode, kann er sich damit anmelden. Wenn ein Benutzer keinen Wiederherstellungscode hat, sollte die Multi-Faktor-Authentifizierung deaktiviert werden, damit sich der Benutzer anmelden und wieder Zugriff erhalten kann.

Um die Multi-Faktor-Authentifizierung eines lokalen Benutzers zu verwalten, muss eine E-Mail-Adresse in derselben Domäne wie der betroffene Benutzer vorhanden sein.

Schritte

1. **Administration** > **Identität und Zugriff** auswählen.
2. **Mitglieder** auswählen.
3. Navigieren Sie auf der Mitgliederseite zu einem Mitglied in der Tabelle, wählen Sie ••• und dann **Multi-Faktor-Authentifizierung verwalten** aus.
4. Wählen Sie, ob die MFA-Konfiguration des Benutzers entfernt oder deaktiviert werden soll.

Nachdem Sie fertig sind

Im Revisionsprotokoll lässt sich nachvollziehen, wer den MFA-Zugriff geändert hat, wann die Änderung vorgenommen wurde und ob die Aktion erfolgreich war. "Informationen zur Überprüfung der lokalen Bereitstellungsaktivität der NetApp Console".

Die Anmeldeinformationen für ein Dienstkonto neu erstellen

Sie können neue Zugangsdaten für ein Dienstkonto erstellen, falls Sie diese verlieren oder aktualisieren müssen.

Durch das Erstellen neuer Anmeldeinformationen werden die alten gelöscht. Die alten Anmeldeinformationen können nicht mehr verwendet werden.

Schritte

1. **Administration** > **Identität und Zugriff** auswählen.
2. **Mitglieder** auswählen.
3. In der Tabelle „Mitglieder“ zu einem Dienstkonto navigieren, ••• auswählen und dann **Geheimnisse neu**

erstellen wählen.

4. **Neu erstellen** auswählen.
5. Die Client-ID und das Client-Geheimnis können heruntergeladen oder kopiert werden.

   Die lokale Bereitstellung in der NetApp Console zeigt das Clientgeheimnis nur einmal an. Es empfiehlt sich, das Clientgeheimnis zu kopieren oder herunterzuladen und sicher aufzubewahren.

Referenz

NetApp Console API für lokale Bereitstellung

Verwaltung der NetApp Console lokalen Bereitstellungsorganisation und Flotten-IDs

In der lokalen NetApp Console-Bereitstellung hat Ihre NetApp Console-Organisation einen Namen und eine ID. Ein Name für Ihre Organisation kann gewählt werden, um sie zu identifizieren. Möglicherweise ist auch die Organisations-ID für bestimmte Integrationen erforderlich.

Erforderliche Zugriffsrollen

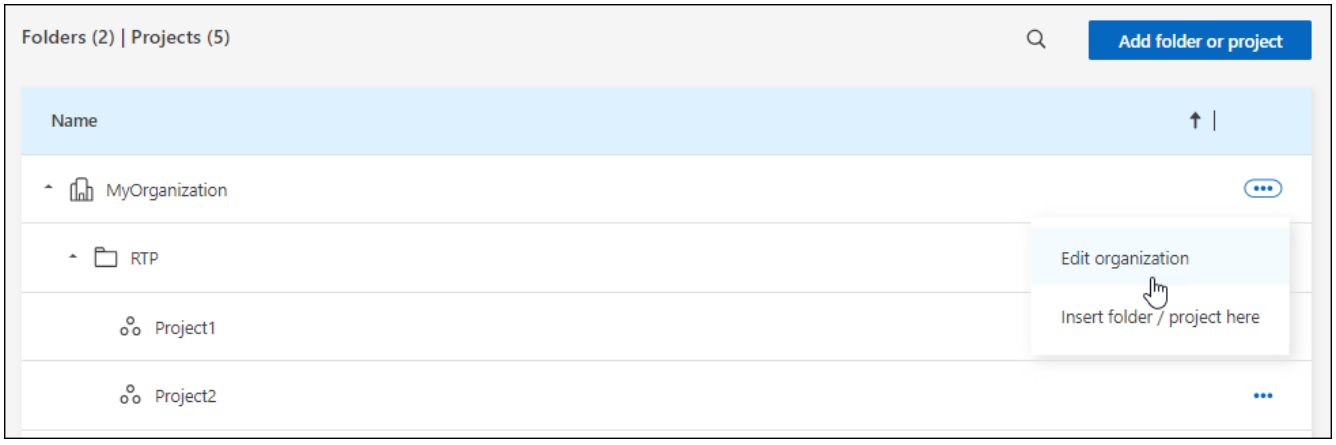
Super Admin oder Organisationsadministrator. "Informationen zu Zugriffsrollen".

Organisation umbenennen

Sie können Ihre Organisation umbenennen.

Schritte

1. **Verwaltung > Identität und Zugriff** auswählen.
2. **Organisation** auswählen.
3. Auf der Seite **Organisation** zur ersten Zeile in der Tabelle navigieren, ••• auswählen und anschließend **Organisation bearbeiten** wählen.



4. Geben Sie einen neuen Organisationsnamen ein und wählen Sie **Anwenden**.

Organisations-ID abrufen

Die Organisations-ID wird für bestimmte Integrationen mit der NetApp Console verwendet.

Die Organisations-ID kann auf der Seite „Organisationen“ angezeigt und für Ihre Zwecke in die Zwischenablage kopiert werden.

Schritte

1. **Verwaltung > Identität und Zugriff** > **Organisation** auswählen.
2. Auf der Seite „Organisation“ befindet sich Ihre Organisations-ID in der Übersichtsleiste und kann in die Zwischenablage kopiert werden. Diese Information lässt sich für eine spätere Verwendung speichern oder direkt an der benötigten Stelle einfügen.

Die ID für eine Flotte abrufen

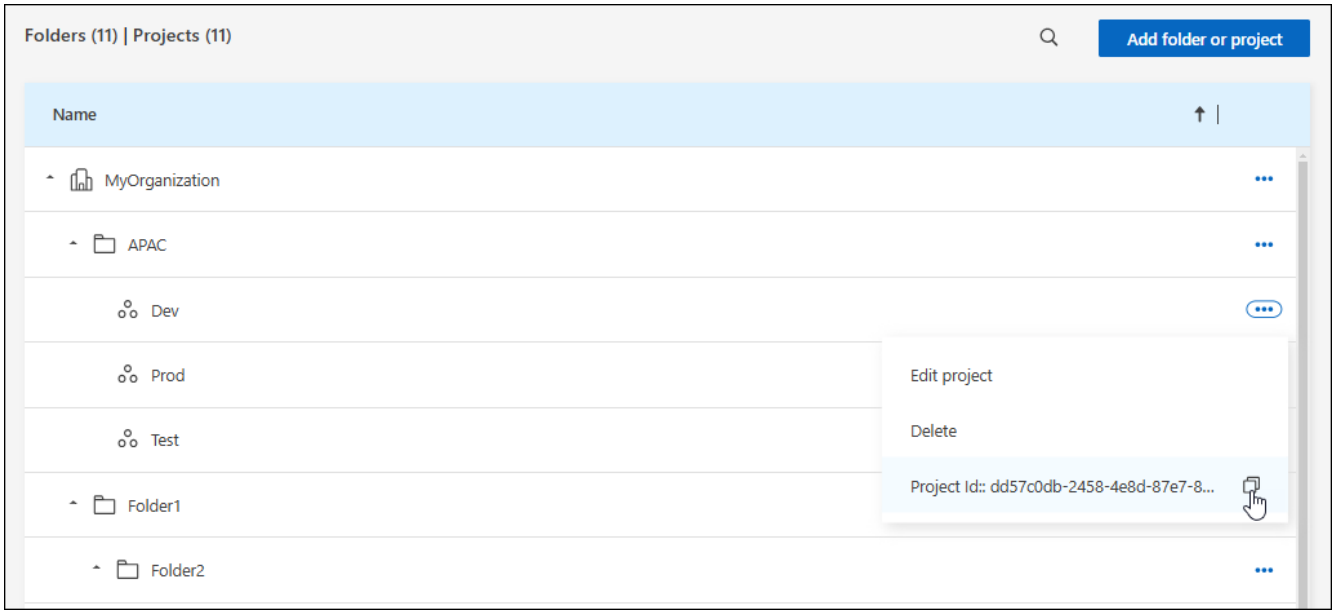
Die ID für eine Flotte ist erforderlich, wenn die API verwendet wird.

Schritte

1. Auf der Seite **Organisation** zu einer Flotte in der Tabelle navigieren und ••• auswählen.

   Die Flotten-ID wird angezeigt.

2. Zum Kopieren der ID die Schaltfläche „Kopieren“ auswählen.



Verwandte Informationen

- "Informationen zu Identitäts- und Zugriffsmanagement"
- "Erste Schritte mit Identität und Zugriff in der NetApp Console"
- "Informationen zur API für Identität und Zugriff"

Unterstützte LLM-Anbieter und Modelle in der lokalen NetApp Console-Bereitstellung

NetApp Console lokale Bereitstellung unterstützt die LLM-Anbietertypen OpenAI, OpenAI-kompatibel und Anthropic. Die Modelle, die ausgewählt werden können, hängen vom Anbietertyp und dem konfigurierten Endpunkt ab.

Diese Dokumentation zur Verbindung eines LLM mit dem Konsolenassistenten zur Aktivierung von KI-Funktionen wird als Technologievorschau bereitgestellt. Mit diesem Vorschauangebot behält sich NetApp das Recht vor, Angebotsdetails, Inhalte und Zeitplan vor der allgemeinen Verfügbarkeit zu ändern.

Wählen Sie ein Modell, das Ihren Leistungs-, Kosten- und Governance-Anforderungen entspricht.

Wie sich der Anbietertyp auf die Modellverfügbarkeit auswirkt

Der gewählte Anbietertyp bestimmt, welche Modelle in der Liste der lokalen Bereitstellungsmodelle der Konsole angezeigt werden:

- **OpenAI** bietet Modelle für die direkte OpenAI Integration.
- **OpenAI-kompatibel** – stellt Modelle bereit, die der kompatible Endpunkt Ihrer Organisation bereitstellt.
- **Anthropic** – bietet Modelle für die direkte Anthropic Integration.

Die angezeigten Modelle können je nach Endpunktkonfiguration, Proxy- oder Gateway-Verhalten und Unternehmensrichtlinie variieren. Anbietertypen unterscheiden sich durch den Endpunkt, mit dem Sie eine Verbindung herstellen, und die von diesem Endpunkt bereitgestellten Modelle, nicht durch das Transportprotokoll.

Unterstützte OpenAI Modelle

- GPT-5.4
- GPT-5.5

Unterstützte Anthropic Modelle

- Claude Sonnet 4.6
- Claude Opus 4.6, 4.7 & 4.8

Verwandte Informationen

- "Verbinden Sie Ihren LLM und aktivieren Sie den NetApp Console Assistenten".
- "Informationen zur LLM-Integration in der lokalen NetApp Console-Bereitstellung".

ONTAP Warnungsreferenz in der NetApp Console lokalen Bereitstellung

Diese Referenz listet die ONTAP-Warnungen auf, die von der lokalen NetApp Console-Bereitstellung überwacht werden können, geordnet nach Auswirkungskategorie.

Schweregradzuordnung

Dieselbe EMS-Warnung kann je nach dem ONTAP-Ereignis, das sie ausgelöst hat, als kritisch, Warnung oder Information erscheinen:

- **Kritisch**: Karten von ONTAP Schweregraden `alert`, `emergency`
- **Warnung**: Zuordnungen vom ONTAP Schweregrad `error`
- **Info**: Karten basierend auf ONTAP Schweregraden `notice`, `informational`

- **Sonstiges**: Unverändert weitergegeben

Durch dynamisches Mapping kann eine einzelne Alarmregel je nach Laufzeitkontext des EMS-Ereignisses unterschiedliche Schweregrade ausgeben.

In den folgenden Abschnitten sind die Warnmeldungen nach Auswirkungskategorie gruppiert und jede Tabelle ist alphabetisch nach Warnmeldungsnamen sortiert.

Verfügbarkeitsbenachrichtigungen

Diese Warnmeldungen können die System-, Service- oder Datenverfügbarkeit beeinträchtigen.

Alarmname	Schwere	Typ	Beschreibung
Verbindung zum Active Directory Server unterbrochen	Kritisch	EMS	Alle für diese SVM konfigurierten AD/LDAP-Server sind nicht erreichbar.
Aggregate ist nicht online	Kritisch	Metrik	Einige Aggregate sind offline. Die Erstellung von Volumes könnte zu doppelten FSIDs führen.
Antivirus Server ausgelastet	Kritisch, Warnung, Info	EMS	Der Antivirenserver ist überlastet und kann keine weiteren Scananfragen annehmen.
AWS-Anmeldeinformationen nicht initialisiert	Kritisch, Warnung, Info	EMS	Ein Modul hat versucht, auf AWS IAM rollenbasierte Anmeldeinformationen zuzugreifen, bevor diese initialisiert wurden.
Cloud-Tier nicht erreichbar	Kritisch, Warnung, Info	EMS	Ein Speicherknoten kann keine Verbindung zur Cloud Tier Objektspeicher API herstellen. Einige Daten sind nicht zugänglich.
Festplattenausfall	Kritisch	Metrik	Eine Festplatte ist ausgefallen, wird bereinigt oder befindet sich im Wartungsmodus.
Festplatte außer Betrieb	Kritisch, Warnung, Info	EMS	Eine Festplatte wurde aufgrund eines Defekts, einer Bereinigung oder Wartungsarbeiten außer Betrieb genommen.
Netzteil der Festplatteneinschübe entfernt	Kritisch, Warnung, Info	EMS	Ein Netzteil wurde aus dem Festplattengehäuse entfernt.
FC-Zielportbefehle überschritten	Kritisch, Warnung, Info	EMS	Die Anzahl der ausstehenden Befehle am physischen FC Zielport überschreitet das unterstützte Limit.
Rückgabe des Speicherpools fehlgeschlagen	Kritisch, Warnung, Info	EMS	Dieses Ereignis tritt während der Verlagerung eines Speicherpools (Aggregats) im Rahmen eines Storage Failover (SFO) Givebacks auf, wenn der Zielknoten die Objektspeicher nicht erreichen kann.
HA Interconnect ausgefallen	Kritisch, Warnung, Info	EMS	Die Hochverfügbarkeitsverbindung (HA-Verbindung) ist ausgefallen. Risiko eines Dienstausfalls, wenn Failover nicht verfügbar ist.

Alarmname	Schwere	Typ	Beschreibung
InstanceDown	Kritisch	Metrik	Die überwachte Instanz ist nicht erreichbar und ist möglicherweise ausgefallen oder es treten Netzwerkprobleme auf.
LUN zerstört	Kritisch, Warnung, Info	EMS	Eine LUN wurde zerstört und ist nicht mehr zugänglich.
LUN offline	Kritisch, Warnung, Info	EMS	Eine LUN wurde manuell offline geschaltet.
Hauptlüfter ausgefallen	Kritisch, Warnung, Info	EMS	Mindestens ein Lüfter der Haupteinheit ist ausgefallen. Das System bleibt betriebsbereit.
Hauptlüfter im Warnzustand	Kritisch, Warnung, Info	EMS	Mindestens ein Lüfter des Hauptgeräts befindet sich im Warnzustand.
Maximale Sitzungsanzahl pro Benutzer überschritten	Kritisch, Warnung, Info	EMS	Sie haben die maximal zulässige Anzahl von Sitzungen pro Benutzer über eine TCP-Verbindung überschritten.
Maximale Anzahl an Dateiöffnungen überschritten	Kritisch, Warnung, Info	EMS	Sie haben die maximale Anzahl an Öffnungen dieser Datei über eine TCP-Verbindung überschritten.
MetroCluster automatische ungeplante Umschaltung deaktiviert	Kritisch, Warnung, Info	EMS	Die automatische ungeplante Umschaltung wurde auf diesem Cluster deaktiviert.
MetroCluster Überwachung	Kritisch, Warnung, Info	EMS	Eine Systemzustandsüberwachungswarnung wurde erkannt.
NFSv4 Speicherpool erschöpft	Kritisch, Warnung, Info	EMS	Ein NFSv4 Store-Pool wurde ausgeschöpft.
NetBIOS Namenskonflikt	Kritisch, Warnung, Info	EMS	Der NetBIOS Name Service hat von einem entfernten Rechner eine negative Antwort auf eine Namensregistrierungsanfrage erhalten.
Keine registrierte Scan-Engine	Kritisch, Warnung, Info	EMS	Der Antivirus-Connector hat ONTAP benachrichtigt, dass keine Scan-Engine registriert ist.
Keine Vscan Verbindung	Kritisch, Warnung, Info	EMS	ONTAP verfügt über keine Vscan Verbindung zur Bearbeitung von Virenscan-Anfragen. Dies kann zu Datenunverfügbarkeit führen, wenn die Option „Scan obligatorisch“ aktiviert ist.
Nicht reagierender Antivirenserver	Kritisch, Warnung, Info	EMS	ONTAP erkannte einen nicht reagierenden Antivirenserver und trennte die Vscan-Verbindung zwangsweise.

Alarmname	Schwere	Typ	Beschreibung
Nicht vorhandene Administratorfreigabe	Kritisch, Warnung, Info	EMS	Vscan-Problem: Ein Client hat versucht, eine Verbindung zu einer nicht existierenden ONTAP_ADMIN$ Freigabe herzustellen.
NVRAM Batterie schwach	Kritisch, Warnung, Info	EMS	Die Kapazität der NVRAM Batterie ist kritisch niedrig. Es kann zu einem potenziellen Datenverlust kommen, wenn die Batterie keinen Strom mehr liefert.
NVMe Namespace zerstört	Kritisch, Warnung, Info	EMS	Ein NVMe Namensraum wurde zerstört und ist nicht mehr zugänglich.
NVMe Namespace offline	Kritisch, Warnung, Info	EMS	Ein NVMe Namespace wurde manuell offline genommen.
NVMe Namespace online	Kritisch, Warnung, Info	EMS	Ein NVMe Namensraum wurde wieder online geschaltet.
NVMe-oF Lizenzkulanzfrist aktiv	Kritisch, Warnung, Info	EMS	Dieses Ereignis tritt täglich auf, wenn das NVMe over Fabrics (NVMe-oF) Protokoll verwendet wird und die Kulanzfrist der Lizenz aktiv ist.
Die Kulanzfrist für die NVMe-oF Lizenz ist abgelaufen.	Kritisch, Warnung, Info	EMS	Die Kulanzfrist für die NVMe over Fabrics (NVMe-oF) Lizenz ist abgelaufen und die NVMe-oF Funktionalität ist deaktiviert.
Beginn der NVMe-oF Lizenzkulanzfrist	Kritisch, Warnung, Info	EMS	Die NVMe over Fabrics (NVMe-oF) Konfiguration wurde während des Upgrades auf ONTAP 9.5 Software erkannt.
Objektspeicher-Host nicht auflösbar	Kritisch, Warnung, Info	EMS	Der Objektspeicher Server-Hostname kann nicht in eine IP-Adresse aufgelöst werden.
Objektspeicher Intercluster-LIF ausgefallen	Kritisch, Warnung, Info	EMS	Der Objektspeicher-Client kann keine betriebsbereite LIF finden, um mit dem Objektspeicher-Server zu kommunizieren.
Signaturkonflikt im Objektspeicher	Kritisch, Warnung, Info	EMS	Die vom Client berechnete Signatur stimmt nicht mit der an den Objektspeicher-Server gesendeten Anforderungssignatur überein.
Portstatus Down	Kritisch	EMS	Dieser Ethernet-Port ist ausgefallen. Der Datenverkehr auf dieser Verbindung kann beeinträchtigt sein.
READDIR Zeitüberschreitung	Kritisch, Warnung, Info	EMS	Ein READDIR-Dateivorgang hat die zulässige Zeitüberschreitung in WAFL überschritten.
Verlagerung des Storage-Pools fehlgeschlagen	Kritisch, Warnung, Info	EMS	Dieses Ereignis tritt während der Verlagerung eines Speicherpools (Aggregat) auf, wenn der Zielknoten die Objektspeicher nicht erreichen kann.

Alarmname	Schwere	Typ	Beschreibung
SAN Aktiv/Aktiv Status geändert	Kritisch, Warnung, Info	EMS	Die SAN-Pfade sind nicht mehr symmetrisch.
Service Processor Heartbeat verpasst	Kritisch, Warnung, Info	EMS	ONTAP empfängt kein erwartetes Heartbeat-Signal vom Service Processor (SP).
Service Processor Heartbeat gestoppt	Kritisch, Warnung, Info	EMS	ONTAP empfängt keine Heartbeats mehr vom Service Processor (SP).
Dienstprozessor nicht konfiguriert	Kritisch, Warnung, Info	EMS	Dieses Ereignis tritt wöchentlich auf, um daran zu erinnern, den Service Processor (SP) zu konfigurieren.
Dienstprozessor offline	Kritisch, Warnung, Info	EMS	Der Service Processor (SP) ist offline.
SFP im FC Zieladapter empfängt geringe Leistung	Kritisch, Warnung, Info	EMS	Diese Warnung tritt auf, wenn die von einem Small Form-Factor Pluggable Transceiver (SFP in FC target) empfangene Leistung (RX) unterhalb des definierten Schwellenwerts liegt.
SFP im FC Zieladapter sendet mit geringer Leistung	Kritisch, Warnung, Info	EMS	Diese Warnung tritt auf, wenn die Sendeleistung (TX) eines Small Form-Factor Pluggable Transceivers (SFP in FC target) unterhalb des definierten Schwellenwerts liegt.
Schattenkopie fehlgeschlagen	Kritisch, Warnung, Info	EMS	Ein Volume Shadow Copy Service (VSS), ein Sicherungs- und Wiederherstellungsdienst von Microsoft Server, ist fehlgeschlagen.
Regallüfter defekt	Kritisch, Warnung, Info	EMS	Der angegebene Lüfter oder das Lüftermodul des Regals ist ausgefallen.
SnapMirror Verzögerungszeit ist hoch	Kritisch	Metrik	Die SnapMirror Beziehung liegt mehr als eine Stunde hinter dem erwarteten Aktualisierungsplan zurück.
Storage Failover Interconnect – Eine oder mehrere Verbindungen ausgefallen	Warnung	EMS	Mindestens eine HA-Interconnect-Verbindung zum Partnerknoten ist ausgefallen. Die Failover-Redundanz ist reduziert.
Netzteile für Storage Switch ausgefallen	Kritisch, Warnung, Info	EMS	Im Cluster-Switch fehlt eine Stromversorgung. Die Redundanz ist reduziert.
Das Anhalten der Storage-VM war erfolgreich.	Kritisch, Warnung, Info	EMS	Die Storage-VM wurde erfolgreich gestoppt.

Alarmname	Schwere	Typ	Beschreibung
SVM Configuration Replication Lizenz ungültig	Warnung	EMS	Die SVM-DR Konfigurationsreplikationslizenz fehlt, ist abgelaufen oder wurde nicht angewendet
Das System kann aufgrund eines Ausfalls des Hauptlüfters nicht betrieben werden.	Kritisch, Warnung, Info	EMS	Mindestens ein Lüfter der Haupteinheit ist ausgefallen, wodurch der Systembetrieb gestört wird. Dies kann zu einem potenziellen Datenverlust führen.
Zu viele CIFS Authentifizierung	Kritisch, Warnung, Info	EMS	Es fanden zahlreiche Authentifizierungsverhandlungen gleichzeitig statt. Von diesem Client liegen 256 unvollständige Anfragen für neue Sitzungen vor.
Nicht zugewiesene Datenträger	Kritisch, Warnung, Info	EMS	Das System verfügt über nicht zugewiesene Festplatten, Kapazität wird verschwendet.
Volume-Status offline	Information en	Metrik	Das Volume wurde offline genommen.
Volume eingeschränkt	Kritisch, Warnung, Info	EMS	Dieses Ereignis zeigt an, dass ein flexibles Volume eingeschränkt wurde.
Virus nachgewiesen	Kritisch, Warnung, Info	EMS	Ein Vscan Server meldete, dass eine Datei möglicherweise mit einem Virus infiziert ist.

Kapazitätswarnungen

Diese Warnmeldungen weisen auf Speicherverbrauch oder Kapazitätsengpässe hin.

Alarmname	Schwere	Typ	Beschreibung
FabricPool Spiegelreplikations-Resynchronisierung abgeschlossen	Kritisch, Warnung, Info	EMS	Der FabricPool Spiegel-Resynchronisierungsprozess wurde erfolgreich vom primären Objektspeicher zum Spiegel-Objektspeicher abgeschlossen.
FabricPool Speicherplatznutzungsgrenze ist fast erreicht	Kritisch, Warnung, Info	EMS	Die gesamte clusterweite FabricPool Speichernutzung der Objektspeicher von Anbietern mit Kapazitätslizenz hat nahezu das lizenzierte Limit erreicht.
FabricPool Auslastungsgrenze erreicht	Kritisch, Warnung, Info	EMS	Die gesamte clusterweite FabricPool Speichernutzung der Objektspeicher von Anbietern mit Kapazitätslizenz hat das Lizenzlimit erreicht.
Root-Volume-Speicherplatz des Knotens niedrig	Kritisch, Warnung, Info	EMS	Das System hat festgestellt, dass der Speicherplatz im Root-Volume gefährlich knapp wird.

Alarmname	Schwere	Typ	Beschreibung
QoS-Monitor-Speicher maximal belegt	Kritisch, Warnung, Info	EMS	Der dynamische Speicher eines QoS-Subsystems hat für die aktuelle Plattformhardware das Limit erreicht.
Automatisches Volume-Resizing erfolgreich	Kritisch, Warnung, Info	EMS	Das Volume wurde automatisch vergrößert, da das automatische Volume-Wachstum aktiviert ist.
Volume voll	Kritisch	Metrik	Das Volume ist zu über 90 % belegt. Speicherplatz kann freigegeben oder die Kapazität erweitert werden, um Schreibfehler zu vermeiden.

Konfigurationswarnungen

Diese Warnmeldungen weisen auf Konfigurationsänderungen oder Bestandsaktualisierungen hin.

Alarmname	Schwere	Typ	Beschreibung
Netzteil für Festplattengehäuse erkannt	Kritisch, Warnung, Info	EMS	Dem Festplattengehäuse wurde ein Netzteil hinzugefügt.
Volume erstellt	Info	Metrik	Ein Volume wurde erstellt.
Volume gelöscht	Warnung	Metrik	Ein Volume wurde gelöscht.
Volume modifiziert	Info	Metrik	Ein Volume wurde geändert.
WAFL Konsistenzprüfung überfällig	Warnung	EMS	WAFL-Konsistenzprüfungen für dieses Aggregat haben das stündliche Limit überschritten.

Leistungswarnungen

Diese Warnmeldungen weisen auf Latenz- oder Knotenleistungsprobleme hin.

Alarmname	Schwere	Typ	Beschreibung
Die NFS-Latenz des Node ist hoch	Kritisch	Metrik	NFS-Operationen auf diesem Knoten weisen eine hohe Latenz auf (>5000 µs).
Knotenpanik	Kritisch, Warnung, Info	EMS	Der Knoten ist ausgefallen und wurde neu gestartet.

Schutzwarnungen

Diese Warnmeldungen betreffen Replikation, Failover oder Wiederherstellung.

Alarmname	Schwere	Typ	Beschreibung
Fanout SnapMirror Beziehung gemeinsamer Snapshot gelöscht	Kritisch, Warnung, Info	EMS	Eine ältere Snapshot-Kopie wird im Rahmen einer SnapMirror synchronen Resynchronisierungs- oder Aktualisierungsoperation gelöscht.
ONTAP Mediator hinzugefügt	Kritisch, Warnung, Info	EMS	Der ONTAP Mediator wurde erfolgreich zu diesem Cluster hinzugefügt.
ONTAP Mediator CA-Zertifikat abgelaufen	Kritisch, Warnung, Info	EMS	Das Zertifikat der Zertifizierungsstelle (CA) des ONTAP Mediator ist abgelaufen.
ONTAP Mediator CA-Zertifikat läuft ab	Kritisch, Warnung, Info	EMS	Das Zertifikat der ONTAP Mediator-Zertifizierungsstelle (CA) läuft innerhalb der nächsten 30 Tage ab.
ONTAP Mediator Clientzertifikat abgelaufen	Kritisch, Warnung, Info	EMS	Das ONTAP Mediator Client-Zertifikat ist abgelaufen.
ONTAP Mediator Clientzertifikat läuft ab	Kritisch, Warnung, Info	EMS	Das ONTAP Mediator Client-Zertifikat läuft innerhalb der nächsten 30 Tage ab.
ONTAP Mediator nicht erreichbar	Kritisch, Warnung, Info	EMS	Der ONTAP Mediator ist nicht zugänglich, entweder weil er umfunktioniert wurde oder weil das Mediator-Paket nicht mehr installiert ist.
ONTAP Mediator entfernt	Kritisch, Warnung, Info	EMS	Der ONTAP Mediator wurde erfolgreich aus diesem Cluster entfernt.
ONTAP Mediator nicht erreichbar	Kritisch, Warnung, Info	EMS	Der ONTAP Mediator ist nicht erreichbar, was bedeutet, dass ein SnapMirror Failover erst möglich ist, wenn die Verbindung wiederhergestellt ist.
ONTAP Mediator Serverzertifikat abgelaufen	Kritisch, Warnung, Info	EMS	Das ONTAP Mediator Serverzertifikat ist abgelaufen.
ONTAP Mediator Serverzertifikat läuft ab	Kritisch, Warnung, Info	EMS	Das ONTAP Mediator Serverzertifikat läuft innerhalb der nächsten 30 Tage ab.
SnapMirror active sync Beziehung ist nicht synchron.	Kritisch, Warnung, Info	EMS	Die SnapMirror synchron Beziehung ist von synchron zu nicht synchron gewechselt. Der Datenschutz ist beeinträchtigt.
SnapMirror active sync automatisches ungeplantes Failover abgeschlossen	Kritisch, Warnung, Info	EMS	Der automatische ungeplante Failover-Vorgang für SnapMirror Business Continuity (SMBC) wurde abgeschlossen.

Alarmname	Schwere	Typ	Beschreibung
SnapMirror active sync automatisches ungeplantes Failover fehlgeschlagen	Kritisch, Warnung, Info	EMS	Der automatische ungeplante Failover-Vorgang für SnapMirror Business Continuity (SMBC) ist fehlgeschlagen.
SnapMirror geplantes Active Sync-Failover abgeschlossen	Kritisch, Warnung, Info	EMS	Der geplante Failover-Vorgang für SnapMirror Business Continuity (SMBC) wurde abgeschlossen.
SnapMirror Active Sync geplantes Failover fehlgeschlagen	Kritisch, Warnung, Info	EMS	Der geplante Failover-Vorgang für SnapMirror Business Continuity (SMBC) ist fehlgeschlagen.
SnapMirror Beziehung gemeinsamer Snapshot fehlgeschlagen	Kritisch, Warnung, Info	EMS	Es ist ein Fehler beim Erstellen einer gemeinsamen Snapshot-Kopie aufgetreten.
SnapMirror Beziehunginitialisierung fehlgeschlagen	Kritisch, Warnung, Info	EMS	Der SnapMirror Initialize-Befehl schlägt fehl und es werden keine weiteren Versuche unternommen.
SnapMirror Beziehung nicht synchron	Kritisch, Warnung, Info	EMS	Die SnapMirror synchron Beziehung ist von synchron zu nicht synchron gewechselt. Der Datenschutz ist beeinträchtigt.
SnapMirror Beziehungssynchronisierungsversuch fehlgeschlagen	Kritisch, Warnung, Info	EMS	Ein SnapMirror Synchronisierungsversuch zwischen Quell- und Zielvolume ist fehlgeschlagen.
SnapMirror Beziehungssnapshot wird nicht repliziert	Kritisch, Warnung, Info	EMS	Die Snapshot-Kopie für die SnapMirror synchron Beziehung wird nicht erfolgreich repliziert.

Sicherheitswarnungen

Diese Warnmeldungen weisen auf Bedrohungen oder unbefugten Zugriff hin.

Alarmname	Schwere	Typ	Beschreibung
Ransomware-Aktivität erkannt	Kritisch, Warnung, Info	EMS	Zum Schutz der Daten vor der erkannten Ransomware wurde eine Snapshot Kopie erstellt, mit der die Originaldaten wiederhergestellt werden können.
Anti-Ransomware-Überwachung für Storage-VMs	Kritisch, Warnung, Info	EMS	Der Anti-Ransomware-Status der Storage VM hat sich geändert.
Unbefugter Benutzerzugriff auf die Administratorfreigabe	Kritisch, Warnung, Info	EMS	Ein Client versuchte, eine Verbindung zur privilegierten Freigabe ONTAP_ADMIN$ herzustellen, aber der angemeldete Benutzer ist nicht Teil eines aktiven Vscan-Scannerpools auf dieser SVM.

Alarmname	Schwere	Typ	Beschreibung
Volume Anti-Ransomware-Überwachung	Kritisch, Warnung, Info	EMS	Der Anti-Ransomware-Status eines Volumes wurde geändert.

Cluster-Sicherheitskonformitätskategorien in der NetApp Console lokalen Bereitstellung

Anhand dieser Referenz lassen sich die in der lokalen NetApp Console-Bereitstellung angezeigten Cluster-Sicherheitskonformitätskategorien einschließlich des empfohlenen Werts und der Information, ob sich die einzelnen Kategorien auf den Gesamtkonformitätsstatus auswirken, überprüfen.

Diese Kategorien basieren auf den Sicherheitsstatusprüfungen von ONTAP.

Kategorie	Was die Kategorie prüft	Empfohlener Wert	Beeinträchtigt die allgemeine Compliance
Globales FIPS	Gibt an, ob der FIPS-140-2-Modus aktiviert ist. Wenn aktiviert, sind TLSv1 und SSLv3 deaktiviert und nur TLSv1.1 und TLSv1.2 zulässig.	Aktiviert	Ja
Telnet	Ob der Telnet-Zugriff aktiviert ist. SSH ist die empfohlene sichere Methode für den Fernzugriff.	Deaktiviert	Ja
Unsichere SSH-Einstellungen	Ob SSH mit unsicheren Verschlüsselungsverfahren konfiguriert ist, wie etwa Verschlüsselungsverfahren, die mit `cbc` beginnen.	Nein	Ja
Anmeldebanner	Ob ein Anmeldebanner für den Systemzugriff konfiguriert ist.	Aktiviert	Ja
Cluster-Peering	Ob die Kommunikation zwischen den verbundenen Clustern verschlüsselt ist. Die Verschlüsselung muss sowohl auf dem Quell- als auch auf dem Zielcluster aktiviert sein.	Verschlüsselt	Ja
Netzwerkzeitprotokoll	Ob ein oder mehrere NTP-Server für den Cluster konfiguriert sind. NetApp empfiehlt mindestens drei NTP-Server für eine hohe Ausfallsicherheit.	Konfiguriert	Ja
OCSP	Ob die Online Certificate Status Protocol Validierung für die SSL/TLS-Zertifikatvalidierung aktiviert ist.	Aktiviert	Nein
Remote-Audit-Protokollierung	Ob die Protokollweiterleitung (syslog) verschlüsselt ist.	Verschlüsselt	Ja
AutoSupport HTTPS-Transport	Ob HTTPS als Standardtransportprotokoll für AutoSupport-Nachrichten verwendet wird.	Aktiviert	Ja
Standard-Admin-Benutzer	Ob das integrierte Standard-Administratorkonto deaktiviert ist.	Deaktiviert	Ja
SAML-Benutzer	Ob SAML für Single Sign-On und MFA-fähige Authentifizierung konfiguriert ist.	Nein	Nein

Kategorie	Was die Kategorie prüft	Empfohlener Wert	Beeinträchtigt die allgemeine Compliance
Active Directory Benutzer	Ob die Active Directory Authentifizierung für den Clusterzugriff konfiguriert ist.	Nein	Nein
LDAP-Benutzer	Ob die LDAP-Authentifizierung für den Clusterzugriff konfiguriert ist.	Nein	Nein
Zertifikatsnutzer	Ob zertifikatbasierte Benutzer für die Clusteranmeldung konfiguriert sind.	Nein	Nein
Lokale Benutzer	Ob lokale Benutzer für die Clusteranmeldung konfiguriert sind.	Nein	Nein
Remote Shell	Ob RSH aktiviert ist. SSH wird für sicheren Fernzugriff bevorzugt.	Deaktiviert	Ja
MD5 wird verwendet	Ob ONTAP Benutzerkonten weiterhin MD5-Hashing anstelle von stärkeren Hashes wie SHA-512 verwenden.	Nein	Ja
Zertifikatsausstellertyp	Der vom Cluster verwendete Zertifikatsausstellertyp.	CA-signiert	Nein

Sicherheitskonformitätskategorien für Storage-VMs in der lokalen NetApp Console-Bereitstellung

Diese Referenz dient zur Überprüfung der in der lokalen NetApp Console-Bereitstellung angezeigten Sicherheitskonformitätskategorien für Storage VMs (SVM), einschließlich des empfohlenen Werts und der Information, ob sich die einzelnen Kategorien auf den Gesamtkonformitätsstatus auswirken.

Diese Kategorien basieren auf den Sicherheitsstatusprüfungen von ONTAP.

Kategorie	Was die Kategorie prüft	Empfohlener Wert	Beeinträchtigt die allgemeine Compliance
Audit-Log	Ob die SVM Audit-Protokollierung aktiviert ist.	Aktiviert	Ja
Unsichere SSH-Einstellungen	Ob SSH mit unsicheren Verschlüsselungsverfahren konfiguriert ist, wie etwa Verschlüsselungsverfahren, die mit `cbc` beginnen.	Nein	Ja
Anmeldebanner	Ob ein Anmeldebanner für Benutzer konfiguriert ist, die auf SVMs zugreifen.	Aktiviert	Ja
LDAP-Verschlüsselung	Ob die LDAP-Verschlüsselung aktiviert ist.	Aktiviert	Nein
NTLM-Authentifizierung	Ob die NTLM-Authentifizierung aktiviert ist.	Aktiviert	Nein
LDAP Nutzlast-Signierung	Ob die LDAP-Nutzlastsignierung aktiviert ist.	Aktiviert	Nein

Kategorie	Was die Kategorie prüft	Empfohlener Wert	Beeinträchtigt die allgemeine Compliance
CHAP-Einstellungen	Ob CHAP aktiviert ist.	Aktiviert	Nein
Kerberos V5	Ob die Kerberos V5 Authentifizierung aktiviert ist.	Aktiviert	Nein
NIS-Authentifizierung	Ob die NIS-Authentifizierung konfiguriert ist.	Deaktiviert	Nein
FPolicy Status aktiv	Ob FPolicy erstellt und aktiv ist.	Ja	Nein
SMB-Verschlüsselung aktiviert	Ob SMB-Signierung und -Versiegelung aktiviert sind.	Ja	Nein
SMB-Signing aktiviert	Ob die SMB-Signierung aktiviert ist.	Ja	Nein

Wissen und Unterstützung

Für Support in der lokalen Bereitstellung der NetApp Console registrieren

NetApp Console lokale Bereitstellungsinformationen für diese Aufgabe. Für den Erhalt von technischem Support speziell für die NetApp Console und deren Storage-Lösungen und Datendienste ist eine Supportregistrierung erforderlich. Eine Supportregistrierung ist ebenfalls erforderlich, um wichtige Workflows für Cloud Volumes ONTAP Systeme zu ermöglichen.

Die Registrierung für den Support aktiviert keinen NetApp Support für einen Dateidienst eines Cloud-Anbieters. Technischer Support in Bezug auf einen Dateidienst eines Cloud-Anbieters, dessen Infrastruktur oder eine Lösung, die diesen Dienst nutzt, ist im Abschnitt „Hilfe erhalten“ der Dokumentation des jeweiligen Produkts zu finden.

- "Amazon FSx for ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Übersicht der Supportregistrierung

Es gibt zwei Registrierungsformen zur Aktivierung des Anspruchs auf Support:

- Registrierung der NetApp Console-Kontoseriennummer (der 20-stellige 960xxxxxxxxx-Seriennummer, die auf der Support Resources-Seite in der Console zu finden ist).

  Dies dient als Ihre einzige Support-Abonnement-ID für jeden Dienst innerhalb der Console. Jedes Console-Konto muss registriert sein.

- Registrierung der Cloud Volumes ONTAP Seriennummern, die mit einem Abonnement verknüpft sind, auf dem Marktplatz Ihres Cloud-Anbieters (dies sind 20-stellige 909201xxxxxxxx Seriennummern).

  Diese Seriennummern werden üblicherweise als *PAYGO-Seriennummern* bezeichnet und von der NetApp Console zum Zeitpunkt der Cloud Volumes ONTAP Bereitstellung generiert.

Durch die Registrierung beider Seriennummerntypen werden Funktionen wie das Erstellen von Support-Tickets und die automatische Fallgenerierung ermöglicht. Die Registrierung wird durch das Hinzufügen von NetApp Support Site (NSS)-Konten zur Konsole abgeschlossen, wie unten beschrieben.

Die NetApp Console für den NetApp Support registrieren

Um sich für den Support zu registrieren und die Supportberechtigung zu aktivieren, muss ein Benutzer Ihres NetApp Console-Kontos ein NetApp Support Site-Konto mit seinem Console-Login verknüpfen. Wie die Registrierung für den NetApp Support erfolgt, hängt davon ab, ob bereits ein NetApp Support Site (NSS)-Konto vorhanden ist.

Bestandskunde mit einem NSS-Konto

Wenn Sie ein NetApp Kunde mit einem NSS-Konto sind, ist lediglich eine Registrierung für den Support über die Console erforderlich.

Schritte

1. **Administration** > **Anmeldeinformationen** auswählen.
2. **Benutzeranmeldeinformationen** auswählen.
3. **NSS-Anmeldeinformationen hinzufügen** auswählen und der Authentifizierungsaufforderung der NetApp Support-Website (NSS) folgen.
4. Zur Bestätigung, dass der Registrierungsvorgang erfolgreich war, das Hilfesymbol auswählen und anschließend **Support** wählen.

   Auf der Seite **Ressourcen** sollte angezeigt werden, dass Ihr Console-Konto für den Support registriert ist.

   Beachten Sie, dass andere Console-Benutzer diesen Support-Registrierungsstatus nicht sehen, wenn sie kein NetApp Support Site-Konto mit ihrem Login verknüpft haben. Das bedeutet jedoch nicht, dass Ihr Konto nicht für den Support registriert ist. Solange mindestens ein Benutzer in der Organisation diese Schritte durchgeführt hat, ist Ihr Konto registriert.

Bestandskunde, aber kein NSS-Konto

Wenn Sie bereits NetApp Kunde sind und über bestehende Lizenzen und Seriennummern, aber *kein* NSS-Konto verfügen, ist es erforderlich, ein NSS-Konto zu erstellen und dieses mit Ihrem Console-Login zu verknüpfen.

Schritte

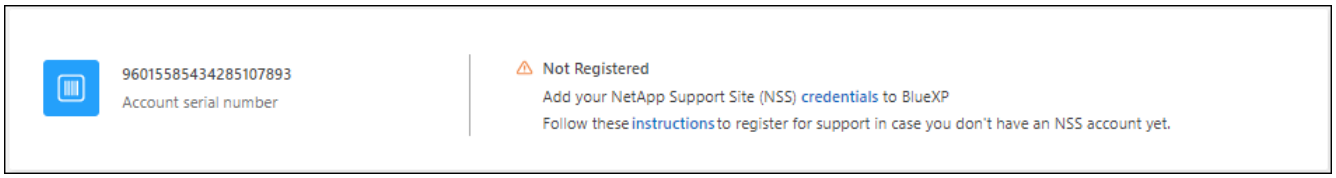
1. Ein NetApp Support Site-Konto kann erstellt werden, indem das "NetApp Support Site Benutzerregistrierungsformular" Formular ausgefüllt wird.
   a. Es sollte die passende Benutzerstufe ausgewählt werden, die in der Regel **NetApp Customer/End User** ist.
   b. Kopieren Sie die oben verwendete Console Account-Seriennummer (960xxxx) für das Seriennummernfeld. Dies beschleunigt die Kontoverarbeitung.
2. Das neue NSS-Konto wird mit Ihrem Console-Login verknüpft, indem die Schritte unter Bestandskunde mit einem NSS-Konto abgeschlossen werden.

Ganz neu bei NetApp

Wenn Sie ganz neu bei NetApp sind und kein NSS-Konto haben, führen Sie die folgenden Schritte aus.

Schritte

1. Oben rechts in der Konsole das Hilfesymbol auswählen und anschließend **Support** wählen.
2. Die Konto-ID-Seriennummer befindet sich auf der Support-Registrierungsseite.



3. Navigieren Sie zu "NetApp's Support-Registrierungsseite" und wählen Sie **Ich bin kein registrierter NetApp Customer** aus.
4. Füllen Sie die Pflichtfelder (die mit roten Sternchen) aus.
5. Im Feld **Produktlinie** wird **Cloud Manager** ausgewählt und anschließend der entsprechende Abrechnungsanbieter.
6. Kopieren Sie Ihre Kontoseriennummer aus Schritt 2 oben, führen Sie die Sicherheitsprüfung durch und bestätigen Sie anschließend, dass Sie die globale Datenschutzrichtlinie von NetApp gelesen haben.

   Um diese sichere Transaktion abzuschließen, wird umgehend eine E-Mail an die angegebene Adresse gesendet. Es empfiehlt sich, den Spam-Ordner zu überprüfen, falls die Bestätigungs-E-Mail nicht innerhalb weniger Minuten eintrifft.

7. Die Aktion wird direkt in der E-Mail bestätigt.

   Mit der Bestätigung wird Ihre Anfrage an NetApp übermittelt und es wird empfohlen, ein NetApp Support Site-Konto zu erstellen.

8. Ein NetApp Support Site-Konto kann erstellt werden, indem das "NetApp Support Site Benutzerregistrierungsformular" Formular ausgefüllt wird.
   a. Es sollte die passende Benutzerstufe ausgewählt werden, die in der Regel **NetApp Customer/End User** ist.
   b. Bitte kopieren Sie die oben angegebene Kontoseriennummer (960xxxx) in das Feld „Seriennummer". Dies beschleunigt die Bearbeitung.

Nachdem Sie fertig sind

NetApp sollte sich während dieses Prozesses mit Ihnen in Verbindung setzen. Dies ist eine einmalige Einführungsmaßnahme für neue Benutzer.

Sobald Sie über Ihr NetApp Support Site-Konto verfügen, kann das Konto mit Ihrem Console-Login verknüpft werden, indem die Schritte unter Bestandskunde mit einem NSS-Konto abgeschlossen werden.

NSS-Zugangsdaten für Cloud Volumes ONTAP Support zuordnen

Die Verknüpfung der NetApp Support Site-Anmeldeinformationen mit Ihrem Console-Konto ist erforderlich, um die folgenden wichtigen Workflows für Cloud Volumes ONTAP zu ermöglichen:

- Registrierung von Cloud Volumes ONTAP Systemen mit nutzungsbasierter Abrechnung für den Support

  Die Angabe Ihres NSS-Kontos ist erforderlich, um den Support für Ihr System zu aktivieren und Zugang zu NetApp technischen Supportressourcen zu erhalten.

- Bereitstellung von Cloud Volumes ONTAP bei Verwendung eigener Lizenz (BYOL)

Die Angabe Ihres NSS-Kontos ist erforderlich, damit die NetApp Console Ihren Lizenzschlüssel hochladen und das Abonnement für die von Ihnen erworbene Laufzeit aktivieren kann. Dies umfasst automatische Updates für Laufzeitverlängerungen.

- Aktualisierung der Cloud Volumes ONTAP Software auf die neueste Version

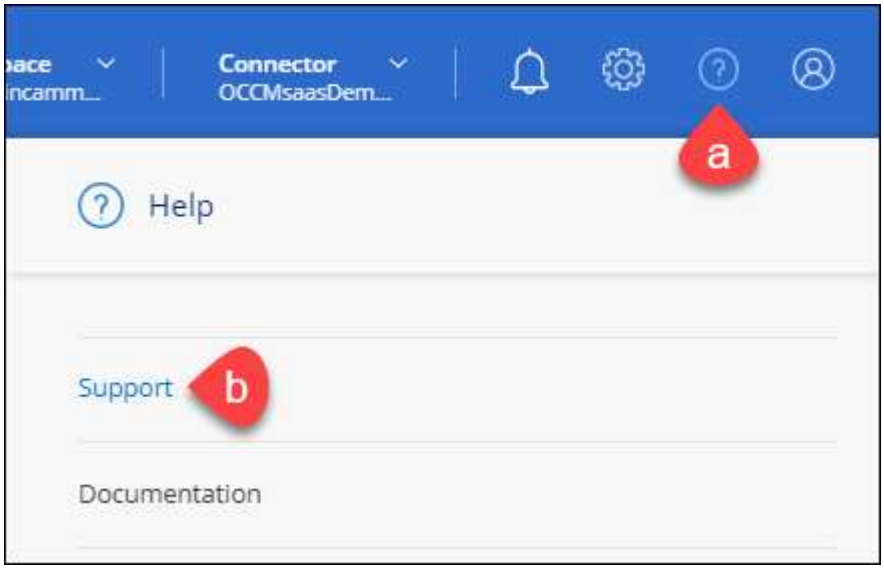
Die Verknüpfung von NSS-Anmeldeinformationen mit Ihrem NetApp Console-Konto unterscheidet sich von dem NSS-Konto, das mit einem Console-Benutzerlogin verknüpft ist.

Diese NSS-Zugangsdaten sind mit Ihrer spezifischen Console-Konto-ID verknüpft. Benutzer, die zur Console-Organisation gehören, können auf diese Zugangsdaten unter **Support > NSS Management** zugreifen.

- Wenn Sie über ein Kundenkonto verfügen, können Sie ein oder mehrere NSS Konten hinzufügen.
- Wenn Sie über ein Partner- oder Reseller-Konto verfügen, können Sie ein oder mehrere NSS-Konten hinzufügen, diese können jedoch nicht zusammen mit Kundenkonten hinzugefügt werden.

Schritte

1. Oben rechts in der Konsole das Hilfesymbol auswählen und anschließend **Support** wählen.



2. **NSS Management > Add NSS Account** auswählen.
3. Wenn Sie dazu aufgefordert werden, **Weiter** auswählen, erfolgt eine Weiterleitung zur Microsoft-Anmeldeseite.

   NetApp verwendet Microsoft Entra ID als Identitätsanbieter für Authentifizierungsdienste im Zusammenhang mit Support und Lizenzierung.

4. Auf der Anmeldeseite sind die bei der NetApp Support Site registrierte E-Mail-Adresse und das Passwort anzugeben, um den Authentifizierungsprozess durchzuführen.

   Diese Aktionen ermöglichen es der Konsole, Ihr NSS-Konto für Aufgaben wie das Herunterladen von Lizenzen, die Überprüfung von Software-Upgrades und zukünftige Support-Registrierungen zu nutzen.

   Dabei ist Folgendes zu beachten:

   - Das NSS-Konto muss ein Kundenkonto sein (kein Gast- oder temporäres Konto). Es können mehrere Kundenkonten auf NSS-Ebene vorhanden sein.

- Es kann nur ein NSS-Konto geben, wenn es sich um ein Partner-Level-Konto handelt. Wenn versucht wird, NSS-Konten auf Kundenebene hinzuzufügen und bereits ein Partner-Level-Konto existiert, erscheint die folgende Fehlermeldung:

  „Der NSS-Kundentyp ist für dieses Konto nicht zulässig, da bereits NSS-Benutzer eines anderen Typs vorhanden sind.“

Das Gleiche gilt, wenn bereits NSS-Kundenkonten vorhanden sind und versucht wird, ein Partnerkonto hinzuzufügen.

- Nach erfolgreicher Anmeldung speichert NetApp den NSS-Benutzernamen.

  Dies ist eine systemgenerierte ID, die Ihrer E-Mail-Adresse zugeordnet ist. Auf der Seite **NSS Management** können Sie Ihre E-Mail-Adresse über das ••• Menü anzeigen.

- Wenn Sie Ihre Anmelde-Credential-Tokens jemals aktualisieren müssen, gibt es im ••• Menü auch die Option **Anmeldeinformationen aktualisieren**.

  Bei Nutzung dieser Option müssen Sie sich erneut anmelden. Beachten Sie, dass das Token für diese Konten nach 90 Tagen abläuft. Eine Benachrichtigung wird veröffentlicht, um Sie darauf hinzuweisen.

Hilfe zur lokalen Bereitstellung der NetApp Console

NetApp Console lokale Bereitstellungsinformationen für diese Aufgabe. NetApp bietet Unterstützung für NetApp Console und dessen Cloud-Services auf vielfältige Weise. Umfangreiche kostenlose Selbsthilfeoptionen wie Knowledge Base (KB)-Artikel und ein Community-Forum stehen rund um die Uhr zur Verfügung. Die Support-Registrierung umfasst technischen Remote-Support über Web-Ticketing.

Support für einen Dateidienst eines Cloud-Anbieters erhalten

Technische Unterstützung im Zusammenhang mit dem Dateidienst eines Cloud-Anbieters, seiner Infrastruktur oder einer Lösung, die diesen Dienst nutzt, finden Sie in der Dokumentation des jeweiligen Produkts.

- "Amazon FSx for ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Um technischen Support speziell für NetApp und dessen Speicherlösungen und Datendienste zu erhalten, nutzen Sie die unten beschriebenen Supportoptionen.

Selbsthilfeoptionen verwenden

Diese Optionen stehen Ihnen kostenlos 24 Stunden am Tag, 7 Tage die Woche zur Verfügung:

- Dokumentation

  Die NetApp Console-Dokumentation, die Sie gerade ansehen.

- "Wissensdatenbank"

  Durchsuchen Sie die NetApp Wissensdatenbank, um hilfreiche Artikel zur Fehlerbehebung zu finden.

- "Communities"

  Tritt der NetApp Console-Community bei, um laufende Diskussionen zu verfolgen oder neue zu starten.

Einen Fall beim NetApp Support erstellen

Zusätzlich zu den oben genannten Selbsthilfeoptionen können Sie nach der Aktivierung des Supports mit einem NetApp Support-Spezialisten zusammenarbeiten, um etwaige Probleme zu lösen.

Bevor Sie beginnen

- Um die Funktion **Fall erstellen** nutzen zu können, müssen Sie zunächst Ihre NetApp Support Site-Anmeldeinformationen mit Ihrem Console-Login verknüpfen. "Erfahren Sie, wie Sie die mit Ihrem Console-Login verknüpften Anmeldeinformationen verwalten.".
- Wenn Sie einen Fall für ein ONTAP System mit Seriennummer eröffnen, muss Ihr NSS-Konto mit der Seriennummer dieses Systems verknüpft sein.

Schritte

1. In der NetApp Console wählen Sie **Hilfe > Support**.
2. Auf der Seite **Ressourcen** steht unter Technischer Support eine der verfügbaren Optionen zur Auswahl:

   a. **Kontaktieren Sie uns** kann ausgewählt werden, wenn ein Telefongespräch mit einer Ansprechperson gewünscht ist. Eine Weiterleitung erfolgt auf eine Seite auf netapp.com, auf der die Telefonnummern aufgeführt sind, die angerufen werden können.

   b. **Fall erstellen** auswählen, um ein Ticket bei einem NetApp Support-Spezialisten zu eröffnen:

      - **Dienst**: Wählen Sie den Dienst aus, dem das Problem zugeordnet ist. Zum Beispiel **NetApp Console**, wenn es sich um ein technisches Supportproblem mit Workflows oder Funktionen innerhalb der Console handelt.
      - **System**: Falls zutreffend, wählen Sie **Cloud Volumes ONTAP** oder **On-Prem** und anschließend die zugehörige Arbeitsumgebung aus.

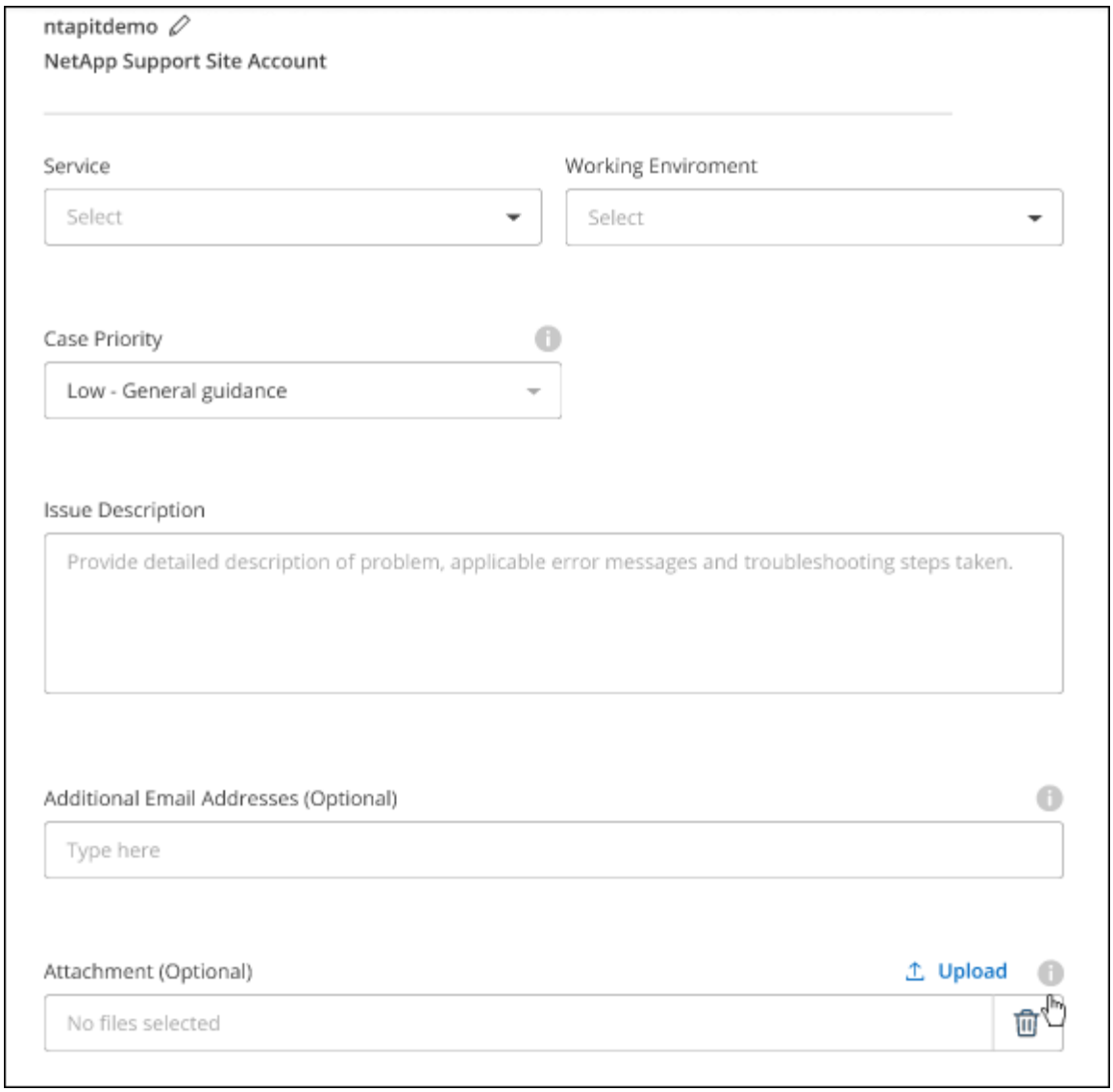
        Die Liste der Systeme befindet sich im Geltungsbereich der Console-Organisation und des Console-Agenten, den Sie im oberen Banner ausgewählt haben.

      - **Fallpriorität**: Die Priorität des Falls kann auf Niedrig, Mittel, Hoch oder Kritisch gesetzt werden.

        Weitere Details zu diesen Prioritäten werden angezeigt, wenn der Mauszeiger über das Informationssymbol neben dem Feldnamen gehalten wird.

      - **Problembeschreibung**: Eine detaillierte Beschreibung des Problems, einschließlich aller relevanten Fehlermeldungen oder durchgeführten Schritte zur Fehlerbehebung.
      - **Weitere E-Mail-Adressen**: Zusätzliche E-Mail-Adressen können eingegeben werden, um eine andere Person auf dieses Problem aufmerksam zu machen.
      - **Anhang (optional)**: Bis zu fünf Anhänge können einzeln hochgeladen werden.

        Anhänge sind auf 25 MB pro Datei beschränkt. Die folgenden Dateierweiterungen werden unterstützt: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx und csv.



Nachdem Sie fertig sind

Es erscheint ein Pop-up mit Ihrer Support-Fallnummer. Ein NetApp Support-Spezialist prüft Ihren Fall und meldet sich in Kürze bei Ihnen.

Für eine Historie Ihrer Supportfälle kann **Einstellungen > Zeitleiste** ausgewählt und nach Aktionen mit dem Namen „Supportfall erstellen“ gesucht werden. Eine Schaltfläche ganz rechts ermöglicht das Erweitern der Aktion, um Details anzuzeigen.

Es ist möglich, dass beim Versuch, einen Fall zu erstellen, die folgende Fehlermeldung angezeigt wird:

„Sie sind nicht berechtigt, einen Case für den ausgewählten Service zu erstellen.“

Dieser Fehler kann bedeuten, dass das NSS-Konto und das zugehörige Unternehmen nicht mit dem Unternehmen übereinstimmen, das für die NetApp Console-Kontoseriennummer (z. B. 960xxxx) oder die Seriennummer der Arbeitsumgebung als Unternehmen der Registrierung geführt ist. Sie können über eine der folgenden Optionen Unterstützung anfordern:

- Einen nicht-technischen Fall einreichen unter https://mysupport.netapp.com/site/help

Verwalten Sie Ihre Supportfälle

Sie können aktive und abgeschlossene Supportfälle direkt in der Console einsehen und verwalten. Sie können die Fälle verwalten, die mit Ihrem NSS-Konto und Ihrem Unternehmen verknüpft sind.

Dabei ist Folgendes zu beachten:

- Das Fallmanagement-Dashboard oben auf der Seite bietet zwei Ansichten:
  - Die Ansicht auf der linken Seite zeigt die Gesamtzahl der in den letzten 3 Monaten über das von Ihnen angegebene NSS-Benutzerkonto eröffneten Fälle.
  - Die Ansicht auf der rechten Seite zeigt die Gesamtzahl der in den letzten 3 Monaten auf Unternehmensebene eröffneten Fälle basierend auf Ihrem NSS-Benutzerkonto.

  Die Ergebnisse in der Tabelle spiegeln die Fälle wider, die sich auf die von Ihnen ausgewählte Ansicht beziehen.
- Sie können Spalten Ihrer Wahl hinzufügen oder entfernen und den Inhalt von Spalten wie Priorität und Status filtern. Andere Spalten bieten lediglich Sortierfunktionen.

  Die folgenden Schritte enthalten weitere Details.
- Auf Ebene einzelner Fälle besteht die Möglichkeit, Fallnotizen zu aktualisieren oder einen Fall zu schließen, der sich noch nicht im Status „Abgeschlossen“ oder „Vorläufig abgeschlossen“ befindet.

Schritte

1. In der NetApp Console wählen Sie **Hilfe > Support**.
2. Wählen Sie **Fallmanagement** aus und fügen Sie gegebenenfalls Ihr NSS-Konto zur Console hinzu.

   Die Seite **Fallverwaltung** zeigt offene Fälle an, die mit dem NSS-Konto verknüpft sind, das Ihrem Console-Benutzerkonto zugeordnet ist. Dies ist dasselbe NSS-Konto, das oben auf der Seite **NSS management** angezeigt wird.
3. Optional können die in der Tabelle angezeigten Informationen geändert werden:
   - Unter **Fälle der Organisation** auf **Anzeigen** auswählen, um alle mit Ihrem Unternehmen verknüpften Fälle anzuzeigen.
   - Der Datumsbereich kann geändert werden, indem entweder ein genauer Datumsbereich oder ein anderer Zeitraum ausgewählt wird.
   - Der Inhalt der Spalten filtern.
   - Ändern Sie die in der Tabelle angezeigten Spalten, indem Sie auswählen und dann die Spalten wählen, die Sie anzeigen möchten.
4. Verwalten Sie einen bestehenden Fall, indem Sie eine der verfügbaren Optionen auswählen:
   - **Fall ansehen**: Vollständige Details zu einem bestimmten Fall anzeigen.
   - **Fallnotizen aktualisieren**: Zusätzliche Details zu Ihrem Problem können angegeben oder **Dateien hochladen** ausgewählt werden, um bis zu fünf Dateien anzuhängen.

     Anhänge sind auf 25 MB pro Datei beschränkt. Die folgenden Dateierweiterungen werden unterstützt: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx und csv.
   - **Fall schließen**: Geben Sie Einzelheiten dazu an, warum Sie den Fall schließen, und wählen Sie **Fall schließen** aus.