ONTAP-Automatisierung

ONTAP Automation

NetApp
July 19, 2024

Inhalt

ONTAP-Automatisierung

Was ist neu

Neuerungen bei der ONTAP REST-API

NetApp aktualisiert regelmäßig das ONTAP REST API, um Ihnen neue Funktionen, Verbesserungen und Fehlerbehebungen zu bieten.

Lesen Sie auch die "Versionshinweise zu ONTAP" Für weitere Informationen, einschließlich bekannter Einschränkungen oder Probleme.

ONTAP 9.15.1

ONTAP 9.15.1 erweitert weiterhin die Funktionen der ONTAP-REST-API. Das Update für diese Version ist relativ bescheiden und unterstützt zwei neue Funktionen.

NFS über TLS

Mit dieser Funktion stehen drei neue Endpunkte zur Verfügung. Sie können diese API-Aufrufe ausgeben, um alle NFS-over-TLS-Schnittstellen abzurufen, eine bestimmte Schnittstelle anhand der UUID abzurufen und die Konfigurationseigenschaften für eine TLS-Schnittstelle zu aktualisieren. Insgesamt bieten diese API-Aufrufe eine Entsprechung zum Satz von `vserver nfs tls interface` CLI-Befehle.

NFS über TLS ist in ONTAP 9.15.1 als öffentliche Vorschau verfügbar. Diese Funktion wird als Vorschauangebot für Produktions-Workloads mit ONTAP 9.15.1 nicht unterstützt.

Windows-Backup-Anwendungen und Unix-ähnliche Symlinks

Wenn eine Windows-Backup-Anwendung auf einen symbolischen Unix-artigen Link (Symlink) stößt, wird der Link durchlaufen, und die Daten werden von ONTAP zurückgegeben und gesichert. Ab ONTAP 9.15.1 haben Sie auch die Möglichkeit, den Symlink statt der darauf angegebenen Daten zu sichern. Dies kann zu mehreren Vorteilen führen, darunter zu einer verbesserten Performance Ihrer Backup-Applikationen. Der Endpunkt `/protocols/cifs/services/{svm.uuid}` wurde aktualisiert, um den neuen Parameter in das Objekt aufzunehmen `backup-symlink-enabled` `options` .

ONTAP 9.14.1

Die Version ONTAP 9.14.1 enthält mehr als drei Dutzend neue API-Aufrufe, die die Funktionen der ONTAP-REST-API weiter erweitern. Diese Endpunkte unterstützen mehrere neue ONTAP-Funktionen sowie Updates vorhandener Funktionen. Dieser Release konzentriert sich in erster Linie auf Sicherheitsverbesserungen, umfasst aber auch Verbesserungen bei NAS-, QOS- und Performance-Kennzahlen.

Sicherheit

Es gibt zwei wichtige Sicherheitsfunktionen, die mit ONTAP 9.14.1 eingeführt wurden. Open Authorization (OAuth 2.0) ist ein Token-basiertes Framework, mit dem der Zugriff auf Ihre ONTAP Storage-Ressourcen eingeschränkt werden kann. Sie können sie zusammen mit Clients verwenden, die über die REST-API auf ONTAP zugreifen. Die Konfiguration kann mit jeder der ONTAP-Administrationsschnittstellen, einschließlich der REST-API, durchgeführt werden. Die Version ONTAP 9.14.1 enthält zudem Unterstützung für Cisco Duo, das für die zwei-Faktor-Authentifizierung bei SSH-Anmeldungen sorgt. Sie können Duo für den Betrieb auf ONTAP-Cluster- oder SVM-Ebene konfigurieren. Zusätzlich zu diesen beiden neuen Funktionen wurden mehrere Endpunkte hinzugefügt, um die Kontrolle über Ihre Schlüsselspeicher zu verbessern.

FPolicy-persistenter Storage

FPolicy stellt eine Plattform für das ONTAP-Richtlinienmanagement bereit. Es stellt einen Container für die verschiedenen Komponenten oder Elemente, wie z. B. Ereignisse und die Richtlinien-Engine, bereit. Sie können jetzt mit der REST-API einen persistenten Speicher für die ONTAP FPolicy Konfiguration und Ereignisse konfigurieren und verwalten. Jede SVM kann über einen persistenten Speicher verfügen, der für mehrere Richtlinien in der SVM freigegeben wird.

QOS-Optionen

Es wurden zwei Endpunkte eingeführt, mit denen Sie QOS-Optionen für das Cluster abrufen und festlegen können. Sie können beispielsweise einen Prozentsatz der verfügbaren Systemverarbeitungsressourcen für Hintergrundaufgaben reservieren.

Performance-Metriken

ONTAP speichert statistische Informationen über die Betriebseigenschaften des Systems. Diese Informationen werden in einem Datenbankformat dargestellt, das aus Tabellen und Zeilen besteht. Mit ONTAP 9.14.1 werden zusätzliche metrische Daten in verschiedenen Ressourcenkategorien hinzugefügt, darunter Fibre Channel, iSCSI, LUNs und NVME. Durch diese zusätzlichen Kennzahlen rückt die ONTAP-REST-API weiterhin näher an die Parität mit der Data ONTAP-API (ONTAPI oder ZAPI) heran.

Verschiedene Verbesserungen

Es gibt mehrere weitere Verbesserungen, die in Abhängigkeit von Ihrer Umgebung hilfreich sein können. Diese neuen Endpunkte verbessern den Zugriff auf die SAN-Initiatoren, die Steuerung der Host-Cache-Einstellungen sowie den Zugriff auf einzelne AutoSupport-Nachrichten.

ONTAP 9.13.1

Mit mehr als zwei Dutzend neuer API-Aufrufe erweitert ONTAP 9.13.1 weiterhin die Funktionen der ONTAP-REST-API. Diese Endpunkte unterstützen neue ONTAP-Funktionen sowie Verbesserungen vorhandener Funktionen. Dieser Release konzentriert sich auf Verbesserungen bei Sicherheit, Ressourcenmanagement, erweiterte SVM-Konfigurationsoptionen und Performance-Kennzahlen.

Ressourcen-Tagging

Sie können Tags verwenden, um REST-API-Ressourcen zu gruppieren. Auf diese Weise können Sie verwandte Ressourcen innerhalb eines bestimmten Projekts oder einer bestimmten Organisationsgruppe zuordnen. Mithilfe von Tags können Sie Ressourcen effektiver organisieren und verfolgen.

Konsistenzgruppen

ONTAP 9.13.1 erweitert weiterhin die Verfügbarkeit von Leistungszählerdaten. Sie können nun auf diese Art von statistischen Informationen zugreifen, um die historische Leistung und Kapazität von Consistency Groups zu verfolgen. Darüber hinaus wurden Verbesserungen integriert, die es ermöglichen, die Beziehungen zwischen übergeordneten und untergeordneten Gruppen zwischen Konsistenzgruppen zu konfigurieren und zu verwalten.

DNS-Konfiguration pro SVM

Die vorhandenen DNS-Endpunkte wurden erweitert, um die Ausführung einer DNS-Domänen- und Serverkonfiguration für einzelne SVMs zu ermöglichen.

EMS-Rollenkonfiguration

Die bestehende EMS-Support-Funktion wurde erweitert, um die Verwaltung von Rollen und die den Rollen zugewiesene Zugangskontrollkonfiguration zu ermöglichen. Dies bietet die Möglichkeit, die Ereignisse und Meldungen basierend auf der Rollenkonfiguration zu begrenzen oder zu filtern.

Sicherheit

Sie können die REST-API verwenden, um die zeitbasierten TOTP-Profile (One-Time Password) für Konten zu konfigurieren, die sich über SSH anmelden und auf ONTAP zugreifen. Darüber hinaus wurden die Schlüsselmanager-Endpunkte erweitert, um eine Wiederherstellung von einem bestimmten Schlüsselmanagementserver aus zu ermöglichen.

CIFS-Konfiguration pro SVM

Die vorhandenen CIFS-Endpunkte wurden erweitert, um eine Aktualisierung der Konfiguration einer spezifischen SVM zu ermöglichen.

S3-Bucket-Regeln

Die bestehenden S3-Bucket-Endpunkte wurden erweitert und um eine Regeldefinition erweitert. Jede Regel ist ein Listenobjekt und definiert die Aktionen, die für ein Objekt innerhalb des Buckets ausgeführt werden sollen. Gemeinsam ermöglichen diese Regeln ein besseres Management des Lebenszyklus von S3 Buckets.

ONTAP 9.12.1

ONTAP 9.12.1 erweitert mit über vierzig neuen API-Aufrufen kontinuierlich die Funktionen der ONTAP REST-API. Diese Endpunkte unterstützen neue ONTAP-Funktionen sowie Verbesserungen vorhandener Funktionen. In dieser Version stehen Verbesserungen bei den Sicherheits- und NAS-Funktionen im Mittelpunkt.

Verbesserte Sicherheit

Amazon Web Services umfasst einen Verschlüsselungsmanagement-Service, der sicheren Storage für Schlüssel und andere Geheimnisse bietet. Sie können über die REST-API auf diesen Service zugreifen, sodass ONTAP seine Schlüssel sicher in der Cloud speichern kann. Darüber hinaus können Sie die mit NetApp Storage Encryption verwendeten Authentifizierungsschlüssel erstellen und auflisten.

Active Directory

Sie können die für ein ONTAP-Cluster definierten Active Directory-Konten verwalten. Dies umfasst das Erstellen neuer Konten sowie das Anzeigen, Aktualisieren und Löschen von Konten.

CIFS-Gruppenrichtlinien

DIE REST-API wurde erweitert, um die Erstellung und das Management von CIFS-Gruppenrichtlinien zu unterstützen. Die Konfigurationsinformationen sind verfügbar und über Gruppenrichtlinienobjekte verwaltet, die auf alle oder bestimmte SVMs angewendet werden.

ONTAP 9.11.1

ONTAP 9.11.1 erweitert weiterhin die Funktionen der ONTAP REST API mit nahezu hundert neuen API-Aufrufen. Diese Endpunkte unterstützen die neuen ONTAP-Funktionen sowie Verbesserungen vorhandener Funktionen. Dieses Release konzentriert Data ONTAP sich darauf, die Migration von Kunden auf die ONTAP REST API (ONTAPI oder ZAPI) zu unterstützen.

Granulare RBAC

Die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) von ONTAP wurde verbessert und bietet nun zusätzliche Granularität. Über die REST-API können Sie je nach Bedarf die herkömmlichen Rollen verwenden oder neue benutzerdefinierte Rollen erstellen. Jede Rolle ist mit einem oder mehreren Berechtigungen verknüpft. Jede Rolle identifiziert einen REST-API-Aufruf oder einen CLI-Befehl zusammen mit der Zugriffsebene. Neue Zugriffsebenen sind für REST-Rollen wie z. B. verfügbar `read_create` Und `read_modify`. Diese Verbesserung bietet Parität mit der Data ONTAP API (ONTAPI oder ZAPI) und unterstützt die Datenmigration in DIE REST API. Siehe "RBAC-Sicherheit" Finden Sie weitere Informationen.

Performance-Zähler

Frühere ONTAP-Releases haben statistische Informationen über die betrieblichen Eigenschaften des Systems erhalten. In der Version 9.11.1 wurden diese Informationen verbessert und sind nun über DIE REST API verfügbar. Ein Administrator oder automatisierter Prozess kann auf die Daten zugreifen, um die Systemleistung zu ermitteln. Die vom Zählermanager-Subsystem aufgesetzten statistischen Informationen werden anhand von Tabellen und Zeilen in einem Datenbankformat dargestellt. Diese Verbesserung bringt das ONTAP REST API näher an Parität mit dem Data ONTAP API (ONTAPI oder ZAPI).

Aggregatmanagement

Das Management von ONTAP-Storage-Aggregaten wurde verbessert. Mithilfe der aktualisierten REST-Endpunkte können Aggregate online und offline verschoben oder die Reserveteile gemanagt werden.

IP-Subnetz-Funktion

Die ONTAP-Netzwerkfunktion wurde erweitert und unterstützt nun IP-Subnetze. Die REST-API bietet Zugriff auf die Konfiguration und das Management der IP-Subnetze innerhalb eines ONTAP-Clusters.

Verifizierung mehrerer Administratoren

Die Überprüfungsfunktion für mehrere Administratoren stellt ein flexibles Autorisierungs-Framework zum Schutz des Zugriffs auf ONTAP-Befehle oder -Vorgänge bereit. Sie können Regeln definieren, die die eingeschränkten Befehle identifizieren. Wenn ein Benutzer Zugriff auf einen bestimmten Befehl anfordert, kann die Genehmigung gegebenenfalls von mehreren ONTAP Administratoren erteilt werden.

SnapMirror Verbesserungen

Die SnapMirror Funktion wurde in verschiedenen Bereichen verbessert, darunter auch die Zeitplanung. Die SnapVault-Beziehungsparität wurde in einer DP-Beziehung zu ONTAP 9.11.1 hinzugefügt auch, die Drosselfunktion, die mit DEM REST API verfügbar ist, hat Parität mit dem Data ONTAP API (ONTAPI oder ZAPI) erreicht. In diesem Zusammenhang wird das Erstellen und Verwalten von Snapshot-Kopien für große Mengen unterstützt.

Storage-Pools

Es wurden mehrere Endpunkte hinzugefügt, um den Zugriff auf die ONTAP Storage-Pools zu ermöglichen. Das Erstellen und Auflisten der Speicherpools in einem Cluster sowie das Aktualisieren und Löschen bestimmter Pools nach ID werden unterstützt.

Name Services Cache Support

ONTAP Name Services wurden erweitert und unterstützen Cache-Speicherung, wodurch Performance und Ausfallsicherheit verbessert werden. Die Konfiguration des Cache für Namensservices kann nun über DIE REST-API aufgerufen werden. Die Einstellungen können auf mehreren Ebenen angewendet werden, darunter Hosts, unix-Benutzer, unix-Gruppen und Netgroups.

ONTAPI Reporting Tool

Das ONTAPI Reporting Tool unterstützt Kunden und Partner bei der Identifizierung der ONTAPI-Nutzung in ihrer Umgebung. Neben der Python Software bietet das NetApp Lab on Demand außerdem ein Video und einen weiterentwickelten Support. Dieses Tool bietet eine weitere Ressource bei der Migration von ONTAPI zu ONTAP REST API.

ONTAP 9.10.1

ONTAP 9.10.1 erweitert weiterhin die Funktionen der ONTAP REST API. Mehr als hundert neue Endpunkte unterstützen neue ONTAP-Funktionen und Verbesserungen vorhandener Funktionen. Im Folgenden finden Sie eine Zusammenfassung der Verbesserungen DER REST API.

Anwendungskonsistenzgruppe

Eine Konsistenzgruppe ist ein Satz von Volumes, die zusammen gruppiert werden, wenn bestimmte Vorgänge wie beispielsweise ein Snapshot durchgeführt werden. Diese Funktion erweitert dieselbe Crash-Konsistenz und Datenintegrität einschließlich Single-Volume-Vorgängen über einen Satz von Volumes hinweg. Dies ist nützlich für Applikationen mit mehreren Volumes.

SVM-Migration

Sie können eine SVM von einem Quell-Cluster zu einem Ziel-Cluster migrieren. Die neuen Endpunkte bieten vollständige Kontrolle, einschließlich der Möglichkeit, den Migrationsvorgang anzuhalten, fortzusetzen, den Status abzurufen und einen Migrationsvorgang abzubrechen.

Klonen und Managen von Dateien

Das Klonen und Managen von Dateien auf Volume-Ebene wurden verbessert. Neue REST-Endpunkte unterstützen das Verschieben, Kopieren und Aufteilen von Dateien.

Verbessertes S3-Auditing

Das Auditing von S3-Ereignissen ist eine Verbesserung der Sicherheit, die es ermöglicht, bestimmte S3-Ereignisse zu verfolgen und zu protokollieren. Ein S3-Audit-Ereigniswähler kann auf Bucket-Basis pro SVM festgelegt werden.

Verteidigung von Ransomware

ONTAP erkennt Dateien, die möglicherweise eine Ransomware-Bedrohung enthalten. Sie können eine Liste dieser verdächtigen Dateien abrufen oder von einem Volume entfernen.

Verschiedene Verbesserungen der Sicherheit

Es gibt verschiedene allgemeine Sicherheitsverbesserungen, durch die vorhandene Protokolle erweitert und neue Funktionen eingeführt werden. IPSEC, Verschlüsselungsmanagement, SSH-Konfiguration und Dateiberechtigungen wurden verbessert.

CIFS-Domänen und lokale Gruppen

Auf Cluster- und SVM-Ebene wurde Unterstützung für CIFS-Domänen hinzugefügt. Sie können die Domänenkonfiguration abrufen sowie bevorzugte Domänen-Controller erstellen und entfernen.

Erweiterte Volume-Analysen

Volume-Analysen und Metriken wurden um zusätzliche Endpunkte erweitert, um Top-Dateien, Verzeichnisse und Benutzer zu unterstützen.

Support-Verbesserungen

Der Support wurde durch mehrere neue Funktionen verbessert. Mit dem automatischen Update können Sie Ihre ONTAP Systeme auf dem neuesten Stand halten, indem Sie die neuesten Software-Updates herunterladen und anwenden. Sie können auch die von einem Node generierten Memory Core Dumps abrufen und verwalten.

ONTAP 9.9.1

ONTAP 9.9.1 erweitert weiterhin die Funktionen der ONTAP REST API. Es gibt neue API-Endpunkte für vorhandene ONTAP Funktionen, einschließlich SAN-Port-Sets und der Sicherheit des Dateiverzeichnisses von Vserver. Außerdem wurden Endpunkte hinzugefügt, um neue ONTAP 9.9.1-Funktionen und -Verbesserungen zu unterstützen. Und auch die dazugehörige Dokumentation wurde verbessert. Im Folgenden finden Sie eine Zusammenfassung der Verbesserungen.

Zuordnen von ONTAPI zu ONTAP 9 REST API

Um den ONTAP-Automatisierungscode in DIE REST-API zu überführen, bietet NetApp Dokumentation zur API-Zuordnung. Diese Referenz enthält eine Liste der ONTAPI-Aufrufe und das entsprechende Rest-API-Äquivalent für jede. Das Zuordnungsdokument wurde aktualisiert und umfasst nun auch die neuen ONTAP 9.9.1 API-Endpunkte. Siehe "ONTAPI-to-REST-API-Zuordnung" Finden Sie weitere Informationen.

API-Endpunkte für neue ONTAP 9.9.1 Kernfunktionen

Unterstützung für neue Funktionen von ONTAP 9.9.1, die nicht über die ONTAPI API verfügbar sind, wurde der REST API hinzugefügt. Dazu gehört auch die Unterstützung für verschachtelte Initiatorgruppen und Google Cloud Key Management Services.

Verbesserte Unterstützung für den Übergang von ONTAPI zu REST

Mehr der bisherigen ONTAPI-Aufrufe haben jetzt entsprechende REST-API-Entsprechungen. Dies umfasst lokale Unix-Benutzer und -Gruppen, Management von NTFS-Dateisicherheit ohne Client-, SAN-Port-Sets und Volume-Speicherplatzattribute. Diese Änderungen sind auch in der aktualisierten ONTAPI to REST Mapping Dokumentation enthalten.

Verbesserte Online-Dokumentation

Die Referenzseite für die ONTAP Online-Dokumentation enthält nun Etiketten, die das ONTAP-Release angeben, wenn jeder REST-Endpunkt oder Parameter eingeführt wurde, einschließlich neuer mit ONTAP 9.9.1.

ONTAP 9.8

ONTAP 9.8 erweitert die Breite und Tiefe der ONTAP REST API. Sie umfasst mehrere neue Funktionen, die Ihre Fähigkeit verbessern, die Implementierung und das Management von ONTAP Storage-Systemen zu automatisieren. Außerdem wurde der Support verbessert, um den Übergang von der älteren ONTAPI zu REST zu unterstützen.

Zuordnen von ONTAPI zu ONTAP 9 REST API

Um Sie bei der Aktualisierung Ihrer ONTAPI-Automatisierung zu unterstützen, bietet NetApp eine Liste von ONTAPI-Aufrufen, die einen oder mehrere Eingabeparameter benötigen, und eine Zuordnung dieser Aufrufe zu dem entsprechenden ONTAP 9 REST API-Aufruf. Siehe "ONTAPI-to-REST-API-Zuordnung" Finden Sie weitere Informationen.

API-Endpunkte für neue ONTAP 9.8 Kernfunktionen

Die Unterstützung für die neuen Core-Funktionen von ONTAP 9.8, die nicht über ONTAPI verfügbar sind, wurde der REST API hinzugefügt. Dazu gehören REST-API-Unterstützung für ONTAP S3-Buckets und -Services, SnapMirror Business Continuity und Dateisystemanalysen.

Erweiterte Unterstützung für erhöhte Sicherheit

Die Sicherheit wurde durch die Unterstützung mehrerer Services und Protokolle verbessert, darunter Azure Key Vault, Google Cloud Key Management Services, IPSec und Certificate Signing Requests.

Erweiterungen zur Verbesserung der Einfachheit

ONTAP 9.8 ermöglicht effizientere und moderne Workflows mithilfe der REST-API. Oneclick Firmware-Updates stehen jetzt beispielsweise für verschiedene Arten von Firmware zur Verfügung.

Verbesserte Online-Dokumentation

Auf der Seite ONTAP Online-Dokumentation sind nun Etiketten mit ONTAP-Version enthalten, die jeden REST-Endpunkt oder Parameter eingeführt wurden, einschließlich der neuen Version in 9.8.

Verbesserte Unterstützung für den Übergang von ONTAPI zu REST

Weitere ältere ONTAPI-Aufrufe haben jetzt entsprechende REST-API-Entsprechungen. Es steht auch eine Dokumentation zur Verfügung, mit der ermittelt werden kann, welcher REST-Endpunkt anstelle eines bestehenden ONTAPI-Aufrufs verwendet werden soll.

Erweiterte Performance-Metriken

Die Performance-Kennzahlen für DIE REST-API wurden auf mehrere neue Storage- und Netzwerkobjekte erweitert.

ONTAP 9.7

ONTAP 9.7 erweitert den Funktionsumfang der ONTAP REST API, indem es drei neue Ressourcenkategorien einführt, jede mit mehreren REST-Endpunkten:

- NDMP
- Objektspeicher
- SnapLock

ONTAP 9.7 führt außerdem einen oder mehrere neue REST-Endpunkte in mehrere bestehende Ressourcenkategorien ein:

- Cluster
- NAS
- Netzwerkbetrieb
- NVMe
- San
- Sicherheit
- Storage
- Unterstützung

ONTAP 9.6

ONTAP 9.6 erweitert die URSPRÜNGLICH in ONTAP 9.4 eingeführte REST-API-Unterstützung enorm. Die ONTAP 9.6 REST API unterstützt die meisten ONTAP Konfigurations- und Administrationsaufgaben.

REST APIs in ONTAP 9.6 enthalten die folgenden und viele mehr:

- Cluster-Einrichtung
- Protokollkonfiguration
- Bereitstellung
- Performance Monitoring
- Datensicherung
- Applikationsspezifisches Datenmanagement

Los geht’s

ONTAP-Automatisierungsoptionen

Es stehen verschiedene Optionen zur Verfügung, um die Implementierung und Administration Ihrer ONTAP Storage-Systeme zu automatisieren.

ONTAP REST API

Ab ONTAP 9.6 bietet ONTAP eine umfassende REST-API, die die Grundlage für die Automatisierung der Implementierung und Administration Ihrer Storage-Systeme bietet. Seitdem hat sich die REST-API weiter erweitert und weiterentwickelt. Sie bietet jetzt die bevorzugte und strategische Option zur Automatisierung der Administration Ihrer ONTAP-Implementierungen.

Nativer Zugriff auf die REST-API

Sie können über jede Programmiersprache, die einen REST-Client unterstützt, direkt auf die ONTAP REST-API zugreifen. Beliebte Sprachen sind Python, PowerShell und Java.

Migration von veraltetem ONTAPI Code zur Nutzung von REST

Die ONTAPI API (Zephyr API oder ZAPI) ist die ursprüngliche Gruppe proprietärer Aufrufe, die in der NetApp ONTAP Software enthalten sind, um die Automatisierung Ihrer Storage-Administrations- und Management-Aufgaben zu unterstützen. Die API ist Teil der "NetApp Manageability SDK". Es wird erwartet, dass die ONTAPI Schnittstelle in zukünftigen Versionen von ONTAP deaktiviert wird. Wenn Sie bereits über Code verfügen, der die ONTAPI API verwendet, sollten Sie eine Migration von ONTAPI planen. NetApp bietet Unterstützung für die Konvertierung Ihres Codes zur Verwendung der neueren ONTAP-REST-API. Siehe "Migrieren Sie von ONTAPI zur REST-API" Finden Sie weitere Informationen.

Toolkits für Clientsoftware

NetApp bietet Client-Toolkits, die die ONTAP-REST-API abstrahieren und die Erstellung von Automatisierungscode vereinfachen. Sie sollten eine geeignete für Ihre Entwicklungssprache und -Umgebung wählen.

Python-Client-Bibliothek

Die Python-Client-Bibliothek ist ein Paket, das beim Schreiben von Skripten für den Zugriff auf die ONTAP REST-API verwendet werden kann. Es unterstützt mehrere zugrunde liegende Services, darunter Verbindungs-Management, asynchrone Anfragebearbeitung und Ausnahmebehandlung. Mithilfe der Python-Client-Bibliothek können Sie schnell robusten Code entwickeln, der Ihre ONTAP-Automatisierungsziele unterstützt. Siehe "Python-Client-Bibliothek" Finden Sie weitere Informationen.

PowerShell Toolkit

Mit dem NetApp.ONTAP PowerShell Toolkit können Sie die Administration eines ONTAP Clusters von einem Windows Host aus automatisieren. Siehe "Überblick über das PowerShell Toolkit" Finden Sie weitere Informationen.

Automatisierungs-Frameworks

Sie können Automatisierungscode mit einem von mehreren Frameworks erstellen und bereitstellen

Ansible

Ansible ist ein Open-Source-Software-Tool, das Bereitstellung, Konfigurationsmanagement und

Applikationseinsatz unterstützt. Seit der Veröffentlichung und der anschließenden Akquisition durch RedHat hat sich diese Beliebtheit stetig weiter entwickelt. NetApp bietet Ansible-zertifizierte Module, mit denen Kunden die Administration ihrer ONTAP Storage-Systeme automatisieren können. Siehe "Weitere Informationen ." Und "NetApp Ansible DevOps-Lösungen" Finden Sie weitere Informationen.

BlueXP Automatisierungskatalog

Das NetApp "BlueXP Automatisierungskatalog" Ist über die BlueXP Web-Benutzeroberfläche verfügbar. Der Katalog bietet Zugriff auf Lösungspakete, mit deren Hilfe Sie die Implementierung und Integration von ONTAP in andere Produkte automatisieren können. Siehe "NetApp-Automatisierung" Für Dokumentation und weitere Informationen.

So erhalten Sie Zugriff auf die ONTAP REST API

Sie können auf die ONTAP REST API auf unterschiedliche Weise zugreifen.

Netzwerküberlegungen

Sie können über folgende Schnittstellen eine Verbindung zur REST API herstellen:

- Cluster-Management-LIF
- Node Management-LIF
- SVM-Management-LIF

Die logische Schnittstelle, die Sie verwenden möchten, muss zur Unterstützung des HTTPS-Managementprotokolls konfiguriert sein. Außerdem muss die Firewall-Konfiguration in Ihrem Netzwerk den HTTPS-Datenverkehr ermöglichen.

Sie sollten immer eine Cluster-Management-LIF verwenden. Dadurch werden die API-Anforderungen über alle Nodes verteilt und Knoten, die offline sind oder Konnektivitätsprobleme haben, werden vermieden. Wenn Sie mehrere Cluster-Management-LIFs konfiguriert haben, entsprechen diese alle dem Zugriff auf die REST-API.

Online-Dokumentationsseite der ONTAP API

Die Online-Dokumentationsseite der ONTAP-API bietet einen Zugriffspunkt bei Verwendung eines Webbrowsers. Die Seite bietet nicht nur die Möglichkeit, einzelne API-Aufrufe direkt auszuführen, sondern enthält auch eine detaillierte Beschreibung der API, einschließlich Eingabeparameter und anderer Optionen für jeden Aufruf. Die API-Aufrufe sind in funktionale Kategorien unterteilt. Siehe "Zusammenfassung der REST-Ressourcen" Finden Sie weitere Informationen.

Das Format der URL, die zum Zugriff auf die Dokumentationsseite der neuesten Version der API verwendet wird, lautet:

```
https://<cluster_mgmt_ip_address>/docs/api
```

Benutzerdefinierte Software und Tools

Sie können auf die ONTAP-API über eine von mehreren verschiedenen Programmiersprachen und Tools zugreifen. Beliebte Optionen sind Python, Java, Curl und PowerShell. Ein Programm, Skript oder Tool, das die API verwendet, fungiert als REST-Web-Services-Client. Die Verwendung einer Programmiersprache ermöglicht ein tieferes Verständnis der API und bietet die Möglichkeit, die ONTAP-Administration zu

automatisieren.

Das Format der Basis-URL, die für den direkten Zugriff auf die neueste Version der API verwendet wird, lautet:

```
https://<cluster_mgmt_ip_address>/api
```

Um auf eine bestimmte API-Version zuzugreifen, in der mehrere Versionen unterstützt werden, lautet das Format der URL:

```
https://<cluster_mgmt_ip_address>/api/v1
```

Ihr erster API-Aufruf

Sie können einen einfachen Curl-Befehl ausgeben, um die ONTAP REST-API zu verwenden und die Verfügbarkeit zu bestätigen.

Bevor Sie beginnen

Neben der Verfügbarkeit des Curl-Dienstprogramms auf Ihrer Workstation benötigen Sie Folgendes:

- IP-Adresse oder FQDN der ONTAP Cluster-Management-LIF
- ONTAP-Anmeldedaten für ein Konto mit einer Berechtigung für den Zugriff auf die ONTAP-REST-API

> Wenn Ihre Anmeldeinformationen Sonderzeichen enthalten, müssen Sie sie entsprechend der verwendeten Shell formatieren. Sie können beispielsweise vor jedem Sonderzeichen einen umgekehrten Schrägstrich einfügen oder die gesamte Zeichenfolge der Anmeldeinformationen in doppelte Anführungszeichen umbrechen.

Schritte

1. Geben Sie an der Befehlszeilenschnittstelle Ihrer lokalen Arbeitsstation den folgenden Befehl ein:

```
curl --request GET \
"https://$FQDN_IP/api/cluster?fields=version" \
--user username:password
```

Beispiel

```
curl --request GET "https://10.29.186.132/api/cluster?fields=version" --user
admin:david123
```

Nachdem Sie fertig sind

Die Informationen zur ONTAP-Version werden in einem JSON-Format angezeigt.

NetApp Lab-Ressourcen

NetApp stellt eine Lab-Umgebung bereit, in der Sie die ONTAP REST-API und andere damit verbundene Automatisierungstechnologien testen können.

Der "Lab on Demand" Steht NetApp Kunden und Partnern zur Verfügung. Sie benötigen gültige

Anmeldeinformationen, um sich anzumelden und die Laborressourcen zu nutzen. Sie können das Labor nach *REST* oder anderen Technologien durchsuchen.

Überprüfen Sie auch "Lab on Demand wird vorbereitet, um die Beispielskripte auszuführen" Und legen Sie los.

ONTAP REST API

Einzelheiten zur REST-Implementierung

REST-Web-Services-Grundlage

Representational State Transfer (REST) ist ein Stil für die Erstellung von verteilten Web-Anwendungen. Bei der Anwendung auf das Design einer Web-Services-API stellt sie eine Reihe von Technologien her, mit denen Server-basierte Ressourcen offengelegt und deren Status verwaltet werden können. Die flexible Grundlage für die Administration von ONTAP Clustern bildet mit Mainstream-Protokollen und -Standards.

IM RUHEZUSTAND werden einheitliche Technologien und Best Practices festgelegt, jedoch können die Details jeder API je nach den während der Entwicklung getroffenen Entscheidungen variieren. Vor der Verwendung mit einer Live-Implementierung sollten Sie sich mit den Designeigenschaften der ONTAP REST API bewusst sein.

Ressourcen- und Zustandsdarstellung

Ressourcen sind die Grundkomponenten eines webbasierten Systems. Beim Erstellen einer ANWENDUNG FÜR REST-Webservices umfassen die frühen Designaufgaben Folgendes:

- Identifizierung von System- oder serverbasierten Ressourcen

  Jedes System nutzt und verwaltet Ressourcen. Eine Ressource kann eine Datei-, Geschäftstransaktion-, Prozess- oder Verwaltungseinheit sein. Eine der ersten Aufgaben bei der Entwicklung einer auf REST-Webservices basierenden Applikation ist die Identifizierung der Ressourcen.

- Definition von Ressourcenstatus und zugehörigen Statusoperationen

  Die Ressourcen befinden sich immer in einer endlichen Anzahl von Staaten. Die Zustände sowie die damit verbundenen Operationen, die zur Auswirkung der Statusänderungen verwendet werden, müssen klar definiert werden.

URI-Endpunkte

Jede REST-Ressource muss definiert und über ein gut definiertes Adressierungssystem verfügbar gemacht werden. Die Endpunkte, in denen die Ressourcen gefunden und identifiziert werden, verwenden einen einheitlichen Resource Identifier (URI). Der URI bietet ein allgemeines Framework zum Erstellen eines eindeutigen Namens für jede Ressource im Netzwerk. Der Uniform Resource Locator (URL) ist ein URI-Typ, der mit Webservices zur Identifizierung und zum Zugriff von Ressourcen verwendet wird. Ressourcen werden in der Regel in einer hierarchischen Struktur ausgesetzt, die einem Dateiverzeichnis ähnelt.

HTTP-Meldungen

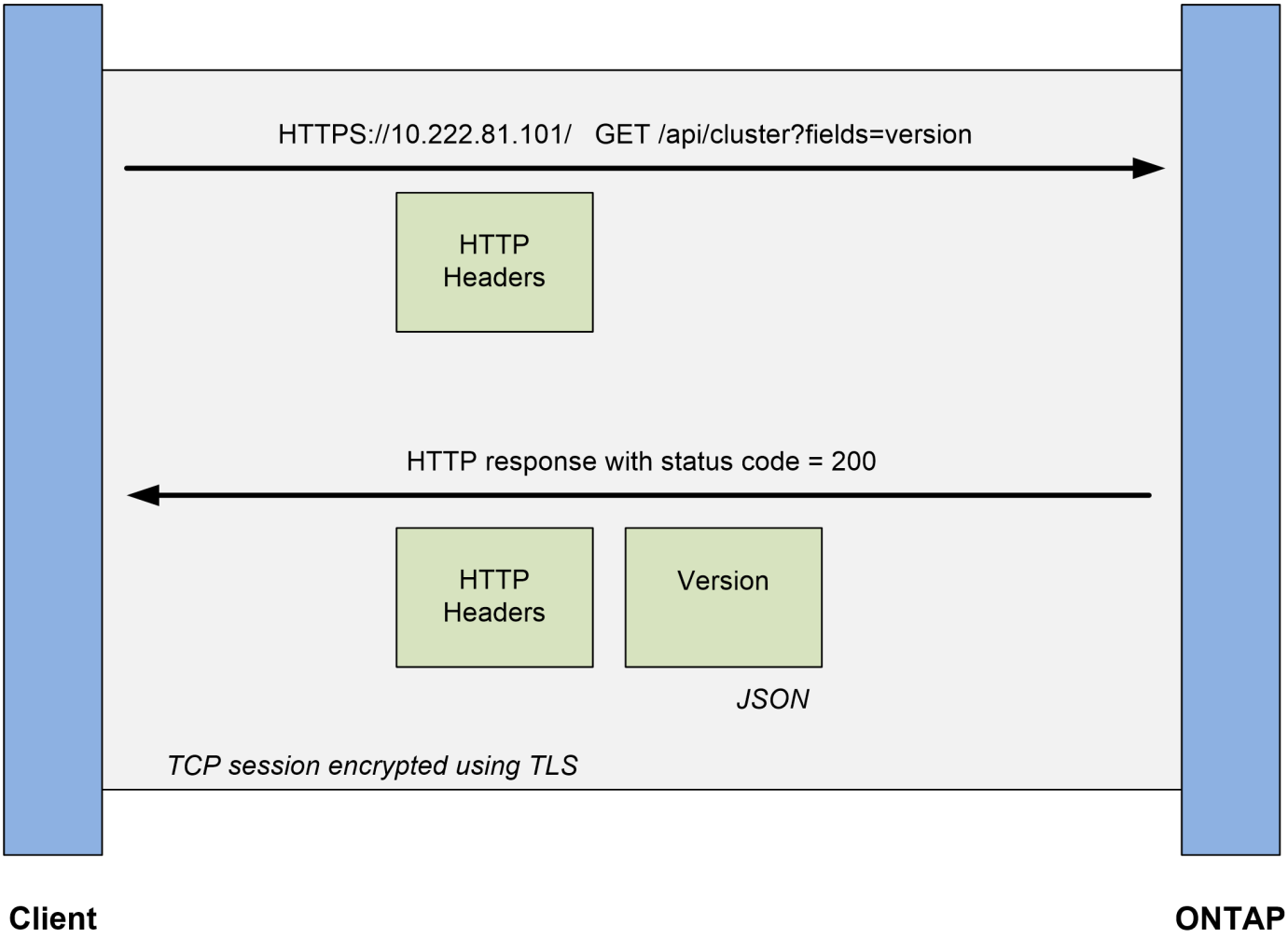
Hypertext Transfer Protocol (HTTP) ist das Protokoll, das vom Webservice-Client und -Server zum Austausch von Anforderungs- und Antwortmeldungen zu den Ressourcen verwendet wird. Im Rahmen der Entwicklung einer Web-Services-Anwendung werden HTTP-Methoden den Ressourcen und entsprechenden Statusmanagement-Aktionen zugeordnet. HTTP ist statusfrei. Um im Rahmen einer Transaktion eine Reihe verwandter Anforderungen und Antworten zuzuordnen, müssen daher zusätzliche Informationen in die HTTP-Header enthalten sein, die mit den Anforderungs- und Antwortdatenströmen verwendet werden.

JSON-Formatierung

Obwohl Informationen auf verschiedene Weise zwischen einem Webservice-Client und Server strukturiert und übertragen werden können, ist die beliebteste Option JavaScript Object Notation (JSON). JSON ist ein Branchenstandard für die Darstellung einfacher Datenstrukturen im Klartext und wird zur Übertragung von Zustandsdaten zur Beschreibung der Ressourcen verwendet. Die ONTAP REST API verwendet JSON, um die Daten zu formatieren, die im Körper jeder HTTP-Anfrage und Antwort verwendet werden.

Typische REST API-Transaktion

Jede API-Transaktion besteht aus einer HTTP-Anfrage und der zugehörigen Antwort. Diese Abbildung zeigt, wie Sie die Version der vom Cluster verwendeten ONTAP Software abrufen können.



HTTP-Anforderung

Die vom Client an den Server gesendete Anforderung besteht aus folgenden Komponenten:

- Verb
- URL-Pfad für das Cluster
- Abfrageparameter (Felder)
- Kopfzeilen für Anfragen, einschließlich Autorisierung

HTTP-Antwort

Die Antwort, die vom Server an den Client gesendet wird, besteht aus folgenden Komponenten:

- Statuscode 200
- Antwortkopfzeilen
- Response Body mit der Cluster-Softwareversion

Grundlegende betriebliche Eigenschaften

IM RUHEZUSTAND werden einheitliche Technologien und Best Practices erstellt, jedoch können die Details jeder API je nach dem verfügbaren Design variieren.

API-Transaktion bei Anfrage und Reaktion

Jeder REST-API-Aufruf wird als HTTP-Anfrage an das ONTAP-System durchgeführt, was eine damit verbundene Antwort an den Client generiert. Dieses Anforderungs-/Antwortpaar wird als API-Transaktion betrachtet. Bevor Sie die API verwenden, sollten Sie mit den verfügbaren Eingabevariablen zur Steuerung einer Anfrage und dem Inhalt der Antwortausgabe vertraut sein.

Unterstützung von CRUD-Vorgängen

Auf alle über das ONTAP REST API verfügbaren Ressourcen kann basierend auf dem CRUD-Modell zugegriffen werden:

- Erstellen
- Lesen
- Aktualisierung
- Löschen

Für einige der Ressourcen wird nur ein Teil der Vorgänge unterstützt. Sie sollten die ONTAP-API-Dokumentationsseite im ONTAP Cluster überprüfen, um weitere Informationen zu jeder Ressource zu erhalten.

Objektkennungen

Jeder Ressourceninstanz oder jedem Objekt wird eine eindeutige Kennung zugewiesen, wenn sie erstellt wird. In den meisten Fällen ist die Kennung eine 128-Bit-UUID. Diese Kennungen sind innerhalb eines bestimmten ONTAP Clusters global eindeutig. Nachdem ein API-Aufruf ausgegeben wurde, der eine neue Objektinstanz erstellt, wird eine URL mit dem zugeordneten id-Wert an den Anrufer im Standortkopf der HTTP-Antwort zurückgegeben. Sie können die Kennung extrahieren und bei nachfolgenden Anrufen verwenden, wenn Sie sich auf die Ressourceninstanz beziehen.

Der Inhalt und die interne Struktur der Objektkennungen können jederzeit geändert werden. Wenn Sie auf die zugeordneten Objekte verweisen, sollten Sie die Kennungen für die entsprechenden API-Aufrufe nur nach Bedarf verwenden.

Objektinstanzen und -Sammlungen

Je nach Ressourcenpfad und HTTP-Methode kann ein API-Aufruf auf eine bestimmte Objektinstanz oder eine Sammlung von Objekten angewendet werden.

Synchroner und asynchroner Betrieb

Es gibt zwei Möglichkeiten, wie ONTAP eine von einem Client empfangene HTTP-Anfrage durchführt.

Synchrone Verarbeitung

ONTAP führt die Anfrage sofort aus und antwortet mit einem HTTP-Statuscode von 200 oder 201, wenn er erfolgreich ist.

Jede Anfrage mit den Methoden GET, HEAD und OPTIONEN wird immer synchron ausgeführt. Darüber hinaus werden Anfragen, die POST, PATCH und LÖSCHEN verwenden, synchron ausgeführt, wenn sie voraussichtlich in weniger als zwei Sekunden abgeschlossen werden.

Asynchrone Verarbeitung

Wenn eine asynchrone Anforderung gültig ist, erstellt ONTAP eine Hintergrundaufgabe zur Verarbeitung der Anforderung und ein Jobobjekt zum Anker der Aufgabe. Der HTTP-Status 202 wird zusammen mit dem Jobobjekt an den Anrufer zurückgegeben. Um den endgültigen Erfolg oder Fehlschlag zu bestimmen, müssen Sie den Status des Jobs abrufen.

Anfragen, die die Methoden POST, PATCH und LÖSCHUNG verwenden, werden asynchron ausgeführt, wenn diese voraussichtlich mehr als zwei Sekunden dauern.

Der `return_timeout` Der Abfrageparameter ist mit asynchronen API-Aufrufen verfügbar und kann einen asynchronen Anruf synchron in den Abschluss konvertieren. Siehe "Asynchrone Verarbeitung mit dem Job-Objekt" Finden Sie weitere Informationen.

Sicherheit

Die Sicherheit der REST-API basiert in erster Linie auf den vorhandenen Sicherheitsfunktionen von ONTAP. Die folgende Sicherheit wird von der API verwendet:

Sicherheit In Transportschicht

Der gesamte über das Netzwerk zwischen dem Client und der logischen Schnittstelle von ONTAP gesendete Datenverkehr wird basierend auf den ONTAP Konfigurationseinstellungen in der Regel mit TLS verschlüsselt.

Client-Authentifizierung

Die gleichen Authentifizierungsoptionen wie bei ONTAP System Manager und dem Network Manageability SDK können auch mit der ONTAP REST API verwendet werden.

HTTP-Authentifizierung

Auf HTTP-Ebene gibt es beispielsweise beim direkten Zugriff auf die ONTAP-REST-API zwei Authentifizierungsoptionen wie unten beschrieben. In jedem Fall müssen Sie einen HTTP-Autorisierungsheader erstellen und diesen bei jeder Anforderung einschließen.

Option	Beschreibung
HTTP-Basisauthentifizierung	Der ONTAP-Benutzername und das Passwort sind mit einem Doppelpunkt verbunden. Der String wird in base64 konvertiert und in den Request Header aufgenommen.
OAuth 2.0	Ab ONTAP 9.14 können Sie ein Zugriffstoken von einem externen Autorisierungsserver anfordern und es als Inhabertoken in den Anforderungsheader aufnehmen.

Weitere Informationen über OAuth 2.0 und die Implementierung in ONTAP finden Sie unter "Überblick über die Implementierung von ONTAP OAuth 2.0". Siehe auch "Die Nutzung der Workflows wird vorbereitet" Unten auf dieser Website.

ONTAP-Autorisierung

ONTAP implementiert ein rollenbasiertes Autorisierungsmodell. Das Konto, das Sie für den Zugriff auf die ONTAP REST-API- oder API-Dokumentationsseite verwenden, sollte über die entsprechende Berechtigung verfügen.

Eingabevariablen, die eine API-Anforderung steuern

Sie können steuern, wie ein API-Aufruf über Parameter und Variablen verarbeitet wird, die in der HTTP-Anforderung festgelegt sind.

HTTP-Methoden

Die von der ONTAP REST API unterstützte HTTP-Methoden sind in der folgenden Tabelle aufgeführt.

Nicht alle HTTP-Methoden sind an jedem REST-Endpunkt verfügbar. AUSSERDEM KÖNNEN PATCH und DELETE für eine Sammlung verwendet werden. Weitere Informationen finden Sie unter *Objektreferenzen und Zugang*.

HTTP-Methode	Beschreibung
GET	Ruft Objekteigenschaften auf einer Ressourceninstanz oder -Sammlung ab.
POST	Erstellt eine neue Ressourceninstanz basierend auf der angegebenen Eingabe.
PATCH	Aktualisiert eine vorhandene Ressourceninstanz basierend auf den eingegebenen Eingaben.
Löschen	Löscht eine vorhandene Ressourceninstanz.
KOPF	Gibt eine GET-Anfrage effektiv aus, gibt aber nur die HTTP-Header zurück.
OPTIONEN	Legen Sie fest, welche HTTP-Methoden an einem bestimmten Endpunkt unterstützt werden.

Pfadvariablen

Der bei jedem REST-API-Aufruf verwendete Endpunktpfad kann verschiedene Kennungen enthalten. Jede ID entspricht einer bestimmten Ressourceninstanz. Beispiele sind Cluster-IDs und SVM-IDs.

Anfragekopfzeilen

Sie müssen mehrere Header in die HTTP-Anfrage aufnehmen.

Inhaltstyp

Wenn der Anforderungsentext JSON enthält, muss dieser Header auf festgelegt werden `application/json`.

Akzeptieren

Diese Kopfzeile sollte auf gesetzt werden `application/hal+json`. Wenn sie stattdessen auf eingestellt ist `application/json` Keiner der HAL-Links wird zurückgegeben, außer ein Link, der zum Abrufen des nächsten Stapels von Datensätzen benötigt wird. Wenn der Header etwas anderes außer diesen beiden Werten ist, ist der Standardwert des `content-type` Die Kopfzeile in der Antwort ist `application/hal+json`.

Autorisierung

Die grundlegende Authentifizierung muss mit dem Benutzernamen und dem Passwort als base64-Zeichenfolge codiert sein. Beispiel:

```
Authorization: Basic YWRtaW46cGV0ZXJzb24=.
```

Text anfordern

Der Inhalt der Anfraentext variiert je nach Anruf. Der HTTP-Request-Text besteht aus einem der folgenden Elemente:

- JSON-Objekt mit Eingabevariablen
- Leeres JSON-Objekt

Objekte filtern

Wenn Sie einen API-Aufruf mit der GET-Methode ausgeben, können Sie die zurückgegebenen Objekte anhand eines beliebigen Attributs mithilfe eines Abfrageparameters einschränken oder filtern.

Analyse und Interpretation von Abfrageparametern

Ein Satz von einem oder mehreren Parametern kann an die URL-Zeichenfolge angehängt werden, die nach dem beginnt `?` Zeichen. Wenn mehrere Parameter angegeben werden, werden die Abfrageparameter auf Basis des aufgeteilt `&` Zeichen. Jede Taste und jeder Wert im Parameter werden am geteilt = Zeichen.

Sie können beispielsweise einen exakten Wert angeben, der mit dem Gleichheitszeichen übereinstimmt:

```
<field>=<value>
```

Für eine komplexere Abfrage wird der zusätzliche Operator nach dem Gleichheitszeichen gesetzt. Um z. B. den Satz von Objekten auf der Grundlage eines bestimmten Felds auszuwählen, der größer oder gleich einem Wert ist, würde die Abfrage folgendermaßen lauten:

```
<field>=>=<value>
```

Filteroperatoren

Zusätzlich zu den oben genannten Beispielen stehen weitere Operatoren zur Verfügung, um Objekte über einen Wertebereich zurückzugeben. Eine Zusammenfassung der von der ONTAP-REST-API unterstützten Filteroperatoren ist in der folgenden Tabelle aufgeführt.

Nicht festgelegte Felder werden in der Regel von übereinstimmenden Abfragen ausgeschlossen.

Operator	Beschreibung
=	Gleich
<	Kleiner als
>	Größer als
<=	Kleiner oder gleich
>=	Größer oder gleich

!	Nicht gleich
*	Gierige Wildcard

Sie können auch eine Sammlung von Objekten zurückgeben, basierend darauf, ob ein bestimmtes Feld über die festgelegt wurde oder nicht `null` Stichwort oder Negation `!null` Als Teil der Abfrage.

Workflow-Beispiele

Einige Beispiele aus den REST-API-Workflows auf dieser Site sind unten aufgeführt.

- "Festplatten auflisten"

  Filter basierend auf dem `state` Variable zur Auswahl der Ersatzfestplatten.

Es werden bestimmte Objektfelder angefordert

Standardmäßig gibt die Ausgabe eines API-Aufrufs mit GET nur die Attribute zurück, die das Objekt oder die Objekte eindeutig identifizieren, zusammen mit einer HAL-Selbstverknüpfung. Dieser minimale Feldsatz dient als Schlüssel für jedes Objekt und variiert je nach Objekttyp. Sie können zusätzliche Objekteigenschaften mithilfe der auswählen `fields` Abfrageparameter auf folgende Weise:

- Allgemeine oder Standardfelder

  Angeben `fields=*` Zum Abrufen der am häufigsten verwendeten Objektfelder. Diese Felder werden normalerweise im lokalen Serverspeicher verwaltet oder erfordern nur wenig Verarbeitung für den Zugriff. Dies sind die gleichen Eigenschaften, die für ein Objekt zurückgegeben werden, nachdem GET mit einem URL-Pfadschlüssel (UUID) verwendet wurde.

- Alle Felder

  Angeben `fields=**` Zum Abrufen aller Objektfelder, einschließlich solcher, die für den Zugriff zusätzliche Serververarbeitung erforderlich sind.

- Benutzerdefinierte Feldauswahl

  Nutzung `fields=<field_name>` Um das genaue Feld anzugeben, das Sie wünschen. Wenn Sie mehrere Felder anfordern, müssen die Werte durch Kommas ohne Leerzeichen getrennt werden.

> Als Best Practice sollten Sie immer die gewünschten Felder identifizieren. Sie sollten nur die gemeinsamen Felder oder alle Felder abrufen, wenn Sie dies benötigen. Welche Felder werden als allgemein klassifiziert und mit zurückgegeben `fields=*`, Wird von NetApp basierend auf interner Performance-Analyse ermittelt. Die Klassifizierung eines Felds kann sich in zukünftigen Releases ändern.

Sortieren von Objekten im Ausgabungsset

Die Datensätze in einer Ressourcensammlung werden in der vom Objekt definierten Standardreihenfolge zurückgegeben. Sie können die Bestellung über ändern `order_by` Abfrage-Parameter mit Feldname und Sortierrichtung wie folgt:

```
order_by=<field name> asc|desc
```

Sie können beispielsweise das Typfeld in absteigender Reihenfolge, gefolgt von id in aufsteigender Reihenfolge sortieren:

```
order_by=type desc, id asc
```

Beachten Sie Folgendes:

- Wenn Sie ein Sortierfeld angeben, aber keine Richtung angeben, werden die Werte in aufsteigender Reihenfolge sortiert.
- Wenn Sie mehrere Parameter eingeben, müssen Sie die Felder mit einem Komma trennen.

Paginierung beim Abrufen von Objekten in einer Sammlung

Wenn ein API-Aufruf über GET auf eine Sammlung von Objekten desselben Typs zugreifen soll, versucht ONTAP, auf der Grundlage von zwei Einschränkungen so viele Objekte wie möglich zurückzugeben. Mit zusätzlichen Abfrageparametern auf der Anforderung können Sie jede dieser Einschränkungen steuern. Die erste Bedingung, die für eine bestimmte GET-Anforderung erreicht wurde, beendet die Anforderung und begrenzt damit die Anzahl der zurückgegebenen Datensätze.

Wenn eine Anfrage endet, bevor sie alle Objekte anführt, enthält die Antwort den Link, der zum Abrufen des nächsten Stapels von Datensätzen benötigt wird.

Die Anzahl der Objekte wird begrenzt

Standardmäßig gibt ONTAP maximal 10,000 Objekte für EINE GET-Anforderung aus. Sie können diese Begrenzung mit dem ändern `max_records` Abfrageparameter. Beispiel:

```
max_records=20
```

Die Anzahl der tatsächlich zurückgegebenen Objekte kann aufgrund der entsprechenden Zeitbeschränkung sowie der Gesamtanzahl der Objekte im System kleiner sein als die maximale Wirkung.

Begrenzung der Zeit, die zum Abrufen der Objekte verwendet wird

Standardmäßig gibt ONTAP so viele Objekte wie möglich innerhalb der für die GET-Anforderung zulässigen Zeit zurück. Die Standard-Zeitüberschreitung beträgt 15 Sekunden. Sie können diese Begrenzung mit dem ändern `return_timeout` Abfrageparameter. Beispiel:

```
return_timeout=5
```

Die Anzahl der tatsächlich zurückgegebenen Objekte kann aufgrund der damit verbundenen Beschränkung auf die Anzahl der Objekte sowie die Gesamtanzahl der Objekte im System kleiner sein als die maximal zulässige Anzahl.

Verengung des Ergebnisset

Bei Bedarf können Sie diese beiden Parameter mit zusätzlichen Abfrageparametern kombinieren, um den Ergebnissatz einzugrenzen. Im Folgenden werden z. B. bis zu 10 ems-Ereignisse zurückgegeben, die nach der angegebenen Zeit generiert wurden:

```
time=> 2018-04-04T15:41:29.140265Z&max_records=10
```

Sie können mehrere Anfragen zur Seite durch die Objekte ausgeben. Jeder nachfolgende API-Aufruf sollte einen neuen Zeitwert verwenden, der auf dem letzten Ereignis des letzten Ergebnisset basiert.

Größeneigenschaften

Die bei einigen API-Aufrufen verwendeten Eingabewerte sowie bestimmte Abfrageparameter sind numerisch. Anstatt eine ganze Zahl in Byte bereitzustellen, können Sie optional ein Suffix wie in der folgenden Tabelle aufgeführt verwenden.

Suffix	Beschreibung
KB	KB-Kilobyte (1024 Byte) oder Kibibyte
MB	MB Megabyte (KB x 1024 Byte) oder Mebibyte
GB	GB Gigabyte (MB x 1024 Byte) oder Gibibyte
TB	TB Terabyte (GB x 1024 Byte) oder Tebibyte
PB	PB (TB x 1024 Byte) oder Pebibyte

Verwandte Informationen

- "Objektreferenzen und -Zugriff"

Interpretation einer API-Antwort

Jede API-Anfrage generiert eine Antwort an den Client. Sie sollten die Antwort überprüfen, um festzustellen, ob sie erfolgreich war, und weitere Daten nach Bedarf abrufen.

HTTP-Statuscode

Im Folgenden werden die von der ONTAP REST API verwendeten HTTP-Statuscodes beschrieben.

Codieren	Grundsatz	Beschreibung
200	OK	Zeigt Erfolg für Anrufe an, die kein neues Objekt erstellen.
201	Erstellt	Ein Objekt wurde erfolgreich erstellt. Der Positionskopf in der Antwort enthält die eindeutige Kennung für das Objekt.
202	Akzeptiert	Ein Hintergrundjob wurde gestartet, um die Anforderung auszuführen, ist aber noch nicht abgeschlossen.
400	Schlechte Anfrage	Die Eingabe der Anfrage ist nicht erkannt oder nicht angemessen.
401	Nicht Autorisiert	Benutzerauthentifizierung fehlgeschlagen.
403	Verboten	Der Zugriff wird aufgrund eines Autorisierungsfehlers verweigert.
404	Nicht gefunden	Die Ressource, auf die in diesem Antrag verwiesen wird, ist nicht vorhanden.
405	Methode nicht zulässig	Die HTTP-Methode in der Anforderung wird für die Ressource nicht unterstützt.
409	Konflikt	Der Versuch, ein Objekt zu erstellen, ist fehlgeschlagen, weil zunächst ein anderes Objekt erstellt werden muss oder das angeforderte Objekt bereits vorhanden ist.
500	Interner Fehler	Ein allgemeiner interner Fehler ist auf dem Server aufgetreten.

Antwortkopfzeilen

In der vom ONTAP erzeugten HTTP-Antwort sind mehrere Header enthalten.

Standort

Wenn ein Objekt erstellt wird, enthält die Standortkopfzeile die komplette URL zum neuen Objekt einschließlich der eindeutigen Kennung, die dem Objekt zugewiesen ist.

Inhaltstyp

Dies ist normalerweise der Fall `application/hal+json`.

Antwortkörper

Der Inhalt des Antwortkörpers, der sich aus einer API-Anfrage ergibt, unterscheidet sich je nach Objekt, Verarbeitungstyp und Erfolg oder Misserfolg der Anforderung. Die Antwort wird immer in JSON gerendert.

- Einzelnes Objekt

  Je nach Anforderung kann ein einzelnes Objekt mit einer Reihe von Feldern zurückgegeben werden. Beispielsweise können Sie GET verwenden, um ausgewählte Eigenschaften eines Clusters mit der eindeutigen Kennung abzurufen.

- Mehrere Objekte

  Es können mehrere Objekte aus einer Ressourcensammlung zurückgegeben werden. In allen Fällen wird ein konsistentes Format verwendet, mit `num_records` Angabe der Anzahl der Datensätze und Datensätze, die ein Array der Objektinstanzen enthalten. Beispielsweise können Sie die in einem bestimmten Cluster definierten Nodes abrufen.

- Jobobjekt

  Wenn ein API-Aufruf asynchron verarbeitet wird, wird ein Job-Objekt zurückgegeben, das den Hintergrund-Task ankers. Beispielsweise wird die PATCH-Anfrage, die zum Aktualisieren der Cluster-Konfiguration verwendet wird, asynchron verarbeitet und ein Job-Objekt zurückgegeben.

- Fehlerobjekt

  Wenn ein Fehler auftritt, wird immer ein Fehlerobjekt zurückgegeben. Beispielsweise erhalten Sie einen Fehler beim Versuch, ein Feld zu ändern, das nicht für ein Cluster definiert ist.

- Leeres JSON-Objekt

  In bestimmten Fällen werden keine Daten zurückgegeben und der Antwortkörper enthält ein leeres JSON-Objekt.

HAL-Verknüpfung

Die ONTAP-REST-API verwendet HAL als Mechanismus zur Unterstützung von Hypermedia als Engine of Application State (HATEOAS). Wenn ein Objekt oder Attribut zurückgegeben wird, das eine bestimmte Ressource identifiziert, wird auch ein HAL-codierter Link enthalten, mit dem Sie einfach weitere Details über die Ressource finden und ermitteln können.

Fehler

Wenn ein Fehler auftritt, wird ein Fehlerobjekt im Antwortkörper zurückgegeben.

Formatieren

Ein Fehlerobjekt hat das folgende Format:

```
"error": {
"message": "<string>",
"code": <integer>[,
"target": "<string>"]
}
```

Sie können den Codewert verwenden, um den allgemeinen Fehlertyp oder die allgemeine Fehlerkategorie zu bestimmen, und die Meldung, um den spezifischen Fehler zu ermitteln. Wenn verfügbar, enthält das Zielfeld die spezifische Benutzereingabe, die mit dem Fehler verknüpft ist.

Allgemeine Fehlercodes

Die gängigen Fehlercodes werden in der folgenden Tabelle beschrieben. Spezifische API-Aufrufe können zusätzliche Fehlercodes enthalten.

Codieren		Beschreibung
1	409	Ein Objekt mit derselben Kennung ist bereits vorhanden.
2	400	Der Wert für ein Feld hat einen ungültigen Wert oder fehlt oder es wurde ein zusätzliches Feld angegeben.
3	400	Der Vorgang wird nicht unterstützt.
4	405	Ein Objekt mit der angegebenen Kennung wurde nicht gefunden.
6	403	Die Berechtigung zur Durchführung der Anforderung wird verweigert.
8	409	Die Ressource wird verwendet.

Asynchrone Verarbeitung mit dem Job-Objekt

Nachdem eine API-Anfrage ausgegeben wurde, die für die asynchrone Ausführung ausgelegt ist, wird immer ein Jobobjekt erstellt und an den Anrufer zurückgegeben. Der Job beschreibt und Anker eine Hintergrundaufgabe, die die Anforderung verarbeitet. Abhängig vom HTTP-Statuscode müssen Sie den Status des Jobs abrufen, um festzustellen, ob die Anforderung erfolgreich war.

Siehe "API-Referenz" Ermitteln, welche API-Aufrufe asynchron ausgeführt werden sollen.

Kontrolle der Verarbeitung einer Anfrage

Sie können das verwenden `return_timeout` Abfrageparameter zur Steuerung der Verarbeitung eines asynchronen API-Aufrufs. Bei Verwendung dieses Parameters sind zwei mögliche Ergebnisse möglich.

Der Timer läuft ab, bevor der Antrag abgeschlossen ist

Bei gültigen Anfragen gibt ONTAP zusammen mit dem Jobobjekt einen HTTP-Statuscode von 202 zurück. Sie müssen den Status des Jobs abrufen, um festzustellen, ob die Anforderung erfolgreich abgeschlossen wurde.

Die Anforderung ist abgeschlossen, bevor der Timer abläuft

Wenn die Anfrage gültig ist und erfolgreich abgeschlossen wird, bevor die Zeit abläuft, gibt ONTAP zusammen mit dem Jobobjekt einen HTTP-Statuscode 200 zurück. Da die Anforderung synchron abgeschlossen wird, wie vom 200 angegeben, müssen Sie den Job-Status nicht abrufen.

Der Standardwert für das `return_timeout` Der Parameter beträgt null Sekunden. Wenn Sie den Parameter nicht angeben, wird der HTTP-Statuscode 202 immer für eine gültige Anfrage zurückgegeben.

Abfragen des mit einer API-Anforderung verknüpften Jobobjekts

Das in der HTTP-Antwort zurückgegebene Job-Objekt enthält mehrere Eigenschaften. Sie können die Statuseigenschaft in einem nachfolgenden API-Aufruf abfragen, um festzustellen, ob die Anforderung erfolgreich abgeschlossen wurde. Ein Job-Objekt befindet sich immer in einem der folgenden Zustände:

Nicht-Terminal-Status

- Warteschlange
- Wird Ausgeführt
- Angehalten

Terminalzustände

- Erfolg
- Ausfall

Allgemeines Verfahren für die Ausgabe einer asynchronen Anfrage

Sie können den folgenden grundlegenden Vorgang verwenden, um einen asynchronen API-Aufruf abzuschließen. In diesem Beispiel wird vorausgesetzt, dass die `return_timeout` Parameter wird nicht verwendet oder die Zeit läuft ab, bevor der Hintergrundjob abgeschlossen ist.

1. Geben Sie einen API-Aufruf aus, der asynchron ausgeführt wird.
2. Sie erhalten eine HTTP-Antwort 202, die auf die Annahme einer gültigen Anfrage hinweist.
3. Extrahieren Sie die Kennung für das Job-Objekt aus dem Antwortkörper.
4. Führen Sie in einem zeitlich festgelegten Regelkreis in jedem Zyklus folgende Schritte aus:
   a. Abrufen des aktuellen Status des Jobs.
   b. Wenn sich der Job nicht im Terminalzustand befindet, führen Sie die Schleife erneut aus.
5. Beenden Sie, wenn der Job einen Terminalstatus erreicht (Erfolg, Fehler).

Verwandte Informationen

- "Cluster-Kontakt aktualisieren"
- "Job-Instanz abrufen"

Objektreferenzen und -Zugriff

Auf die über die ONTAP REST-API offengelegten Ressourceninstanzen oder Objekte kann auf unterschiedliche Weise zugegriffen werden.

Objektzugriffspfade

Auf hoher Ebene gibt es zwei Pfadtypen für den Zugriff auf ein Objekt:

- Primär

  Das Objekt ist das primäre oder direkte Ziel des API-Aufrufs.

- Im Ausland

  Das Objekt ist nicht die primäre Referenz des API-Aufrufs, sondern ist mit dem primären Objekt verknüpft. Es handelt sich daher um ein fremdes oder nachgeschalteter Objekt und wird durch ein Feld im primären Objekt referenziert.

Zugriff auf ein Objekt mithilfe der UUID

Jedem Objekt wird eine eindeutige ID bei der Erstellung zugewiesen. Dies ist in den meisten Fällen eine 128-Bit-UUID. Die zugewiesenen UUID-Werte sind unveränderlich und werden innerhalb von ONTAP intern zum Zugriff und Management der Ressourcen verwendet. Aus diesem Grund bietet die UUID im Allgemeinen die schnellste und stabilste Art, auf Objekte zuzugreifen.

Für viele Ressourcentypen kann ein UUID-Wert als Teil des Pfadschlüssels in der URL bereitgestellt werden, um auf ein bestimmtes Objekt zuzugreifen. Beispielsweise können Sie Folgendes verwenden, um auf eine Node-Instanz zuzugreifen: `/cluster/nodes/{uuid}`

Zugriff auf ein Objekt mithilfe einer Objekteigenschaft

Zusätzlich zu einer UUID können Sie auch mithilfe einer Objekteigenschaft auf ein Objekt zugreifen. In den meisten Fällen ist es bequem, die Namenseigenschaft zu verwenden. Sie können beispielsweise den folgenden Abfrageparameter in der URL-Zeichenfolge verwenden, um auf eine Node-Instanz mit ihrem Namen zuzugreifen: `/cluster/nodes?name=node_one`. Zusätzlich zu einem Abfrageparameter kann über eine Eigenschaft im primären Objekt auf ein fremdes Objekt zugegriffen werden.

Während Sie den Namen oder eine andere Eigenschaft für den Zugriff auf ein Objekt anstelle der UUID verwenden können, gibt es einige mögliche Nachteile:

- Das Namensfeld ist nicht unveränderlich und kann geändert werden. Wenn der Name eines Objekts vor dem Zugriff auf ein Objekt geändert wird, wird das falsche Objekt zurückgegeben oder ein Objektzugriffsfehler schlägt fehl.

  Dieses Problem kann mit EINER POST- oder PATCH-Methode auf einem fremden Objekt oder mit EINER GET-Methode auf einem primären Objekt auftreten.

- ONTAP muss das Namensfeld in die entsprechende UUID übersetzen. Diese Art von indirekten Zugriff kann zu einem Performance-Problem werden.

Insbesondere kann eine Performance-Verschlechterung erzielt werden, wenn eine oder mehrere der folgenden zutrifft:

- GET-Methode wird verwendet
- Auf eine große Sammlung von Objekten wird zugegriffen
- Es wird eine komplexe oder aufwändige Abfrage verwendet

Der Kontext zwischen Cluster und SVM

Es gibt mehrere REST-Endpunkte, die sowohl ein Cluster als auch eine SVM unterstützen. Wenn Sie einen dieser Endpunkte verwenden, können Sie den Kontext des API-Aufrufs über das anzeigen `scope=[svm|cluster]` Wert: Beispiele für Endpunkte, die einen dualen Kontext unterstützen, sind IP-Schnittstellen und Sicherheitsrollen.

Der Scope-Wert hat einen Standardwert, der auf den Eigenschaften basiert, die für jeden API-Aufruf bereitgestellt werden.

VERWENDEN VON PATCHES und LÖSCHEN einer Sammlung von Objekten

Jeder REST-Endpunkt, der PATCH oder LÖSCHUNG auf einer Ressourceninstanz unterstützt, unterstützt auch dieselbe Methode bei einer Objektsammlung. Die einzige Voraussetzung ist, dass mindestens ein Feld über einen Abfrageparameter im URL-String bereitgestellt werden muss. Bei der Ausgabe eines PATCHES oder BEIM LÖSCHEN einer Sammlung entspricht dies dem internen Verfahren:

- Abfrage-basierte ABRUFEN, um die Sammlung abzurufen
- Serielle Sequenz von PATCHES oder LÖSCHANRUFE für jedes Objekt in der Sammlung

Die Zeitdauer für den Vorgang kann von eingestellt werden `return_timeout` Standardmäßig 15 Sekunden. Wenn die Antwort vor dem Timeout nicht abgeschlossen wurde, enthält sie einen Link zum nächsten Objekt. Sie müssen dieselbe HTTP-Methode über den nächsten Link erneut ausgeben, um den Vorgang fortzusetzen.

Performance-Metriken für Storage-Ressourcen

ONTAP sammelt Performance-Kennzahlen zu ausgewählten SVM-Storage-Objekten und -Protokollen und meldet diese Informationen über DIE REST-API. Sie können diese Daten für die Überwachung der Performance eines ONTAP Systems verwenden.

Für ein Storage-Objekt oder ein bestimmtes Protokoll fallen die Performance-Daten in drei Kategorien:

- IOPS
- Latenz
- Durchsatz

Innerhalb jeder Kategorie steht ein oder mehrere der folgenden Datentypen zur Verfügung:

- Lesen ®
- Schreiben (W)
- Sonstiges (O)
- Gesamt (T)

Die folgende Tabelle fasst die Performance-Daten zusammen, die über die ONTAP REST API verfügbar sind, einschließlich des Release, sobald sie hinzugefügt wurde. Weitere Informationen finden Sie auf der REST-API-Online-Dokumentationsseite Ihres ONTAP Systems.

Storage-Objekt oder -Protokoll	IOPS	Latenz	Durchsatz	Version von ONTAP
Ethernet-Anschluss	Keine Angabe	Keine Angabe	RWT	9.8
FC-Port	RWOT	RWOT	RWT	9.8
IP-Schnittstelle	Keine Angabe	Keine Angabe	RWT	9.8
FC-Schnittstelle	RWOT	RWOT	RWT	9.8
NVMe-Namespace	RWOT	RWOT	RWOT	9.8
Qtree-Statistiken	RAW-RWOT	Keine Angabe	RAW-RWOT	9.8
Volume FlexCache	RWOT	RWOT	RWT	9.8
Node – Prozessnutzung	Prozessnutzung als numerischer Wert	Prozessnutzung als numerischer Wert	Prozessnutzung als numerischer Wert	9.8
Cloud Volume	RWOT	RWOT	Nicht applierbar	9.7
LUN	RWOT	RWOT	RWOT	9.7
Aggregat	RWOT	RWOT	RWOT	9.7
NFS-Protokoll der SVM	RWOT	RWOT	RWT	9.7
CIFS-Protokoll für SVM	RWOT	RWOT	RWT	9.7
FCP-Protokoll der SVM	RWOT	RWOT	RWT	9.7
ISCSI-Protokoll der SVM	RWOT	RWOT	RWT	9.7
NVMe-Protokoll der SVM	RWOT	RWOT	RWT	9.7
Cluster	RWOT	RWOT	RWOT	9.6
Volumes	RWOT	RWOT	RWOT	9.6

RBAC-Sicherheit

Überblick über die RBAC-Sicherheit

ONTAP verfügt über eine robuste und erweiterbare Funktion zur rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC). Sie können jedem Konto eine eigene Rolle zuweisen, um den Zugriff des Benutzers auf die Ressourcen zu kontrollieren, die über DIE REST-API und die Rest-CLI offengelegt werden. Die Rollen definieren für verschiedene ONTAP Benutzer verschiedene Zugriffsebenen.

Die RBAC-Funktion von ONTAP wurde kontinuierlich erweitert und in ONTAP 9.11.1 (und nachfolgenden Versionen) deutlich verbessert. Weitere Informationen finden Sie unter "Zusammenfassung der Entwicklung der RBAC" und "Neuerungen bei der ONTAP REST-API" .

ONTAP Rollen

Eine Rolle ist eine Reihe von Berechtigungen, die kollektiv definieren, welche Aktionen der Benutzer ergreifen kann. Jede Berechtigung identifiziert einen bestimmten Zugriffspfad und die zugehörige Zugriffsebene. Rollen werden Benutzerkonten zugewiesen und von ONTAP bei Zugriffskontrollentscheidungen angewendet.

Rollentypen

Es gibt zwei Arten von Rollen. Sie wurden mit der Weiterentwicklung von ONTAP auf verschiedene Umgebungen eingeführt und angepasst.

Bei der Verwendung jeder Rollenart gibt es vor- und Nachteile. Siehe "Vergleichen der Rollentypen" Finden Sie weitere Informationen.

Typ	Beschreibung
RUHE	DIE REST-Funktionen wurden mit ONTAP 9.6 eingeführt und werden in der Regel für Benutzer angewendet, die über DIE REST-API auf ONTAP zugreifen. Durch das Erstellen einer RUHEROLLE wird automatisch eine traditionelle *Mapping*-Rolle erzeugt.
Traditionell	Hierbei handelt es sich um die älteren Rollen, die vor ONTAP 9.6 enthalten sind. Sie wurden für die ONTAP CLI Umgebung eingeführt und sind weiterhin von grundlegender Bedeutung für die RBAC-Sicherheit.

Umfang

Jede Rolle hat einen Umfang oder Kontext, in dem sie definiert und angewendet wird. Der Umfang legt fest, wo und wie eine bestimmte Rolle verwendet wird.

ONTAP-Benutzerkonten haben einen ähnlichen Umfang und bestimmen, wie ein Benutzer definiert und verwendet wird.

Umfang	Beschreibung
Cluster	Rollen mit Clusterumfang werden auf ONTAP Cluster-Ebene definiert. Sie sind mit Benutzerkonten auf Cluster-Ebene verbunden.
SVM	Rollen mit SVM-Umfang werden für eine bestimmte Daten-SVM definiert. Sie sind Benutzerkonten in derselben SVM zugewiesen.

Quelle der Rollendefinitionen

Es gibt zwei Möglichkeiten, wie eine ONTAP-Rolle definiert werden kann.

Rollenquelle	Beschreibung
Individuell	Der ONTAP-Administrator kann benutzerdefinierte Rollen erstellen. Diese Rollen können an eine spezifische Umgebung und Sicherheitsanforderungen angepasst werden.

Rollenquelle	Beschreibung
Integriert	Während individuelle Rollen für mehr Flexibilität sorgen, gibt es auch eine Reihe integrierter Rollen, die sowohl auf Cluster- als auch auf SVM-Ebene verfügbar sind. Diese Rollen sind vordefiniert und können für viele allgemeine administrative Aufgaben verwendet werden.

Rollenzuordnung und ONTAP-Verarbeitung

Abhängig von der verwendeten ONTAP Version werden alle oder fast alle REST-API-Aufrufe einem oder mehreren CLI-Befehlen zugeordnet. Wenn Sie eine RUDERROLLE erstellen, wird auch eine traditionelle oder ältere Rolle erstellt. Diese traditionelle **Mapping** Rolle basiert auf den entsprechenden CLI Befehlen und kann nicht manipuliert oder verändert werden.

Reverse Role Mapping wird nicht unterstützt. Das heißt, die Schaffung einer traditionellen Rolle schafft keine entsprechende RUHEROLLE.

Zusammenfassung der Entwicklung der RBAC

Die herkömmlichen Rollen sind bei allen Versionen von ONTAP 9 enthalten. DIE RESTLICHEN Rollen wurden später eingeführt und haben sich wie unten beschrieben weiterentwickelt.

ONTAP 9.6

DIE REST API wurde mit ONTAP 9.6 eingeführt. IN dieser Version wurden auch die REST-Rollen enthalten. Wenn Sie eine RUSTROLLE anlegen, wird auch eine entsprechende traditionelle Rolle erzeugt.

ONTAP 9.7 bis 9.10.1

Jede ONTAP Version von 9.7 bis 9.10.1 enthält Verbesserungen an DER REST API. So wurden beispielsweise jeder Version weitere REST-Endpunkte hinzugefügt. Die Erstellung und Verwaltung der beiden Rollentypen blieb jedoch getrennt. Zudem wurde in ONTAP 9.10.1 DIE REST-RBAC-Unterstützung für den Rest-Endpunkt von Snapshots hinzugefügt `/api/storage/volumes/{vol.uuid}/snapshots` Bei diesem Punkt handelt es sich um einen ressourcenqualifizierten Endpunkt.

ONTAP 9.11.1

Mit diesem Release wurde die Möglichkeit hinzugefügt, herkömmliche Rollen mit DER REST API zu konfigurieren und zu managen. Weitere Zugriffsebenen für DIE REST-Rollen wurden hinzugefügt.

Arbeiten Sie mit Rollen und Benutzern

Nachdem Sie die grundlegenden RBAC-Funktionen kennen, können Sie sofort mit den ONTAP Rollen und Benutzern arbeiten.

Siehe "RBAC-Workflows" Beispiele für das Erstellen und Verwenden von Rollen mit der ONTAP-REST-API

Administrativen Zugriff

Sie können die ONTAP Rollen über DIE REST-API oder die Befehlszeilenschnittstelle erstellen und managen. Die Zugriffsdetails sind unten beschrieben.

REST API

Es gibt verschiedene Endpunkte, die bei der Arbeit mit RBAC-Rollen und Benutzerkonten verwendet werden können. Die ersten vier in der Tabelle werden zum Erstellen und Verwalten der Rollen verwendet. Die letzten beiden werden zum Erstellen und Verwalten von Benutzerkonten verwendet.

Sie können online auf das ONTAP zugreifen "API-Referenz" Dokumentation Weitere Informationen einschließlich Beispiele für die Verwendung der API.

Endpunkt	Beschreibung
`/security/roles`	Mit diesem Endpunkt können Sie eine neue REST-Rolle erstellen. Ab ONTAP 9.11.1 können Sie auch eine traditionelle Rolle spielen. In diesem Fall bestimmt ONTAP den Rollentyp basierend auf den Eingabeparametern. Sie können auch eine Liste der definierten Rollen abrufen.
`/security/roles/{owner.UUID}/{name}`	Sie können eine bestimmte Cluster- oder SVM-Scoped-Rolle abrufen oder löschen. Der UUID-Wert gibt die SVM an, in der die Rolle definiert ist (Cluster oder Daten-SVM). Der Name ist der Name der Rolle.
`/security/roles/{owner.UUID}/{name}/privileges`	Mit diesem Endpunkt können Sie die Berechtigungen für eine bestimmte Rolle konfigurieren. Die eingebauten Rollen können abgerufen, aber nicht aktualisiert werden. Weitere Informationen finden Sie in der API-Referenzdokumentation für Ihre ONTAP Version.
`/security/roles/{owner.UUID}/{name}/privileges/[path]`	Sie können die Zugriffsebene und den optionalen Abfragewert für eine bestimmte Berechtigung abrufen, ändern und löschen. Weitere Informationen finden Sie in der API-Referenzdokumentation für Ihre ONTAP Version.
`/security/accounts`	Mit diesem Endpunkt können Sie ein neues Benutzerkonto im Umfang des Clusters oder der SVM erstellen. Es müssen mehrere Arten von Informationen enthalten oder anschließend hinzugefügt werden, bevor das Konto betriebsbereit ist. Sie können auch eine Liste der definierten Benutzerkonten abrufen.
`/security/accounts/{owner.UUID}/{name}`	Sie können ein bestimmtes Benutzerkonto mit Cluster oder SVM-Umfang abrufen, ändern und löschen. Der UUID-Wert gibt die SVM an, in der der Benutzer definiert ist (Cluster oder Daten-SVM). Der Name ist der Name des Kontos.

Befehlszeilenschnittstelle

Die entsprechenden ONTAP CLI Befehle werden im Folgenden beschrieben. Auf alle Befehle wird auf der Cluster-Ebene über ein Administratorkonto zugegriffen.

Befehl	Beschreibung
`security login`	Dies ist das Verzeichnis mit den Befehlen, die zum Erstellen und Verwalten einer Benutzeranmeldung benötigt werden.
`security login rest-role`	Dies ist das Verzeichnis mit den Befehlen, die zum Erstellen und Verwalten einer REST-Rolle benötigt werden, die einer Benutzeranmeldung zugeordnet ist.

Befehl	Beschreibung
`security login role`	Dies ist das Verzeichnis mit den Befehlen, die zum Erstellen und Managen einer traditionellen Rolle benötigt werden, die einer Benutzeranmeldung zugeordnet ist.

Rollendefinitionen

DIE REST- und traditionellen Rollen werden durch eine Reihe von Attributen definiert.

Eigentümer und Umfang

Eine Rolle kann im Besitz des ONTAP Clusters oder einer spezifischen Daten-SVM innerhalb des Clusters sein. Der Eigentümer bestimmt auch implizit den Umfang der Rolle.

Eindeutiger Name

Jede Rolle muss einen eindeutigen Namen in ihrem Geltungsbereich haben. Der Name einer Cluster-Rolle muss auf ONTAP Cluster-Ebene eindeutig sein, während die SVM-Rollen innerhalb der spezifischen SVM eindeutig sein müssen.

> Der Name einer neuen REST-Rolle muss sowohl unter DEN REST-Rollen als auch den traditionellen Rollen eindeutig sein. Das liegt daran, dass die Schaffung einer RUHEROLLE auch zu einer neuen traditionellen *Mapping* Rolle mit dem gleichen Namen führt.

Satz von Berechtigungen

Jede Rolle enthält einen Satz von mindestens einer Berechtigung. Jede Berechtigung identifiziert eine bestimmte Ressource oder einen bestimmten Befehl und die zugehörige Zugriffsebene.

Berechtigungen

Eine Rolle kann eine oder mehrere Berechtigungen enthalten. Jede Berechtigungsdefinition ist ein Tupel und legt die Zugriffsebene für eine bestimmte Ressource oder Operation fest.

Ressourcenpfad

Der Ressourcenpfad wird entweder als REST-Endpunkt oder als CLI-Befehl-/Befehlsverzeichnispfad identifiziert.

REST-Endpunkt

Ein API-Endpunkt hat die Zielressource für eine REST-Rolle identifiziert.

CLI-Befehl

Ein CLI-Befehl gibt das Ziel für eine herkömmliche Rolle an. Es kann auch ein Befehlsverzeichnis angegeben werden, das dann alle nachgelagerten Befehle in die ONTAP-CLI-Hierarchie enthält.

Zugangsstufe

Die Zugriffsebene definiert den Zugriffstyp, den die Rolle zum spezifischen Ressourcenpfad oder Befehl hat. Die Zugriffsebenen werden durch eine Reihe vordefinierter Schlüsselwörter identifiziert. Mit ONTAP 9.6 wurden drei Zugriffsebenen eingeführt. Sie können sowohl für traditionelle als auch FÜR REST-Rollen verwendet werden. Darüber hinaus haben ONTAP 9.11.1 drei neue Zugriffsebenen hinzugefügt. Diese neuen Zugriffsebenen können nur mit REST-Rollen verwendet werden.

Die Zugriffsebenen folgen dem CRUD-Modell. Bei REST basiert dies auf den primären HTTP-Methoden (POST, GET, PATCH, DELETE). Die entsprechenden CLI-Vorgänge werden im Allgemeinen den REST-Vorgängen zugeordnet (Erstellen, Anzeigen, Ändern, Löschen).

Zugangsstufe	RUHT primitives	Hinzugefügt	Nur RUSTFUNKTION
Keine	k. A.	9.6	Nein
readonly	GET	9.6	Nein
Alle	ABRUFEN, POSTEN, PATCHEN, LÖSCHEN	9.6	Nein
Read_create	GET, POST	9.11.1	Ja.
Lesen_ändern	GET, PATCH	9.11.1	Ja.
Lesen_create_modify	ABRUFEN, POST, PATCH	9.11.1	Ja.

Optionale Abfrage

Beim Erstellen einer traditionellen Rolle können Sie optional einen **query**-Wert angeben, um die Teilmenge der für das Befehlsverzeichnis oder das Befehlsverzeichnis relevanten Objekte zu identifizieren.

Zusammenfassung der integrierten Rollen

ONTAP enthält verschiedene vordefinierte Rollen, die Sie auf Cluster- oder SVM-Ebene verwenden können.

Cluster-Scoped-Rollen

Im Umfang des Clusters sind verschiedene integrierte Rollen verfügbar.

Siehe "Vordefinierte Rollen für Cluster-Administratoren" Finden Sie weitere Informationen.

Rolle	Beschreibung
Admin	Administratoren mit dieser Rolle haben uneingeschränkte Rechte und können alles im ONTAP-System tun. Sie können alle Ressourcen auf Cluster-Ebene und SVM-Ebene konfigurieren.
AutoSupport	Dies ist eine spezielle Rolle, die speziell auf das AutoSupport-Konto zugeschnitten ist.
Backup	Diese besondere Rolle für Backup-Software, die das System sichern muss.
SnapLock	Dies ist eine spezielle Rolle, die speziell auf das SnapLock-Konto zugeschnitten ist.
readonly	Administratoren mit dieser Rolle können sämtliche Daten auf Cluster-Ebene anzeigen, jedoch keine Änderungen vornehmen.
Keine	Es werden keine Administrationsfunktionen bereitgestellt.

SVM-Scoped-Rollen

Im Umfang der SVM sind verschiedene integrierte Rollen verfügbar. Der **vsadmin** bietet Zugriff auf die allgemeinsten und leistungsfähigsten Funktionen. Es gibt verschiedene zusätzliche Rollen, die auf bestimmte administrative Aufgaben zugeschnitten sind. Dazu zählen:

- Vsadmin-Volume
- Vsadmin-Protokoll
- Vsadmin-Backup
- Vsadmin-snaplock
- Vsadmin-Readonly

Siehe "Vordefinierte Rollen für SVM-Administratoren" Finden Sie weitere Informationen.

Vergleichen der Rollentypen

Bevor Sie eine **REST**-Rolle oder **traditionelle**-Rolle auswählen, sollten Sie sich der Unterschiede bewusst sein. Im Folgenden werden einige Möglichkeiten beschrieben, wie die beiden Rollentypen verglichen werden können.

> Für erweiterte oder komplexere RBAC-Anwendungsfälle sollten Sie normalerweise eine herkömmliche Rolle verwenden.

Wie der Benutzer auf ONTAP zugreift

Vor dem Erstellen einer Rolle ist es wichtig zu wissen, wie der Benutzer auf das ONTAP-System zugreifen kann. Auf dieser Grundlage kann ein Rollentyp ermittelt werden.

Datenzugriff	Vorgeschlagener Typ
Nur REST API	DIE REST-Rolle wurde für die Verwendung mit DER REST-API konzipiert.
REST API UND CLI	Sie können eine RUHEROLLE definieren, die auch eine entsprechende traditionelle Rolle erzeugt.
Nur CLI	Sie können eine traditionelle Rolle erstellen.

Präzision des Zugriffspfads

Der für eine REST-Rolle definierte Zugriffspfad basiert auf einem REST-Endpunkt. Der Zugriffspfad für eine herkömmliche Rolle basiert auf einem CLI-Befehl oder einem Befehlsverzeichnis. Darüber hinaus können Sie einen optionalen Abfrageparameter mit einer traditionellen Rolle hinzufügen, um den Zugriff anhand der Befehlsparameter-Werte weiter zu beschränken.

Zusammenfassung der REST-Ressourcen

Übersicht der Ressourcenkategorien

Die über die ONTAP REST-API verfügbaren Ressourcen sind in Kategorien organisiert. Jede der Ressourcenkategorien enthält eine kurze Beschreibung sowie ggf. weitere Überlegungen zur Nutzung.

Die in der Zusammenfassung beschriebenen REST-Ressourcen basieren auf der neuesten Version des Produkts. Weitere Informationen zu den in früheren Versionen vorgenommenen Änderungen finden Sie unter "Neuerungen bei der ONTAP REST API" Sowie dem "Versionshinweise zu ONTAP".

Für viele DER REST-Endpunkte können Sie einen UUID-Schlüssel als Teil der Pfadzeichenfolge für den Zugriff auf eine bestimmte Objektinstanz enthalten. In vielen Fällen können Sie jedoch auch über einen Eigenschaftswert eines Abfrageparameters auf Objekte zugreifen.

Verwandte Informationen

- "API-Referenz"

Applikation

Sie können diese API-Aufrufe zur Verwaltung der ONTAP-Anwendungsressourcen verwenden.

Applikations-Snapshots

Applikationen unterstützen Snapshot Kopien, die jederzeit erstellt oder wiederhergestellt werden können. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Applikationen Unterstützt

Die ONTAP-Applikationen werden nach Typ angeordnet. Diese umfassen Vorlagen, Applikationen, Komponenten und Snapshot Kopien. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Konsistenzgruppen

Eine Konsistenzgruppe ist ein Satz von Volumes, die zusammen gruppiert werden, wenn bestimmte Vorgänge wie beispielsweise ein Snapshot durchgeführt werden. Diese Funktion erweitert dieselbe Crash-Konsistenz und Datenintegrität einschließlich Single-Volume-Vorgängen über einen Satz von Volumes hinweg. Dieser Ressourcentyp wurde mit ONTAP 9.10 eingeführt und mit 9.12 aktualisiert. Mit ONTAP 9.13 wurde ein Endpunkt zum Abrufen von Performance- und Kapazitätsdaten hinzugefügt.

Snapshots von Konsistenzgruppen

Mit diesen Endpunkten können Snapshots für eine Konsistenzgruppe kopiert, erstellt, inventarisieren und wiederhergestellt werden. Dieser Ressourcentyp wurde mit ONTAP 9.10 eingeführt.

Cloud

Diese API-Aufrufe können zum Managen von Verbindungen zu Objekt-Storage-Ressourcen in der Cloud verwendet werden.

Ziele

Ein Ziel repräsentiert eine Objekt-Storage-Ressource in der Cloud. Jedes Ziel umfasst Konfigurationsinformationen, die für die Verbindung zur Storage-Ressource erforderlich sind. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Cluster

Sie können diese API-Aufrufe verwenden, um ONTAP-Cluster und die zugehörigen Ressourcen zu verwalten.

Kapazitäts-Pools

Mit dem Modell der Kapazitäts-Pools können Sie die Storage-Kapazität für jeden Cluster Node aus einem gemeinsam genutzten Pool lizenzieren. Dieser Ressourcentyp ist neu in ONTAP 9.8.

Chassis

Das Chassis ist das Hardware-Framework, das ein Cluster unterstützt. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Cluster

Ein ONTAP Cluster enthält mindestens einen Knoten sowie die zugehörigen Konfigurationseinstellungen, die das Storage-System definieren. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Zählertabellen

Verschiedene statistische Informationen über ONTAP werden vom Zählermanager-Subsystem erfasst. Sie können auf diese Informationen zugreifen, um die Systemleistung zu bewerten. Dieser Ressourcentyp wurde mit ONTAP 9.11 eingeführt.

Firmware

Sie können einen Verlauf der Firmware-Aktualisierungsanforderungen abrufen. Dieser Ressourcentyp ist neu in ONTAP 9.8.

Jobs

Asynchrone REST-API-Anforderungen werden über eine Hintergrundaufgabe ausgeführt, die durch einen Job verankert ist. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Lizenzinstanz

Jede Lizenz kann als separates Paket gemanagt werden. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Lizenzmanager

Sie können Konfiguration und andere Informationen zu jeder Lizenz-Manager-Instanz, die einem ONTAP-Cluster zugeordnet ist, verwalten. Dieser Ressourcentyp ist neu in ONTAP 9.8.

Lizenzen Zu Haben

Die Lizenzen ermöglichen es Ihnen, spezifische ONTAP Funktionen und Features zu implementieren. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Mediatoren

Sie können den mit MetroCluster verknüpften Mediator verwalten, einschließlich Hinzufügen oder Entfernen der Mediatorinstanz. Dieser Ressourcentyp ist neu in ONTAP 9.8.

MetroCluster

Sie können eine MetroCluster Implementierung erstellen und managen, einschließlich dem Ausführen von Switchover- oder Switchback-Vorgängen. Dieser Ressourcentyp ist neu in ONTAP 9.8 und aktualisiert mit 9.11.

MetroCluster Diagnose

Sie können einen Diagnosevorgang bei einer MetroCluster-Bereitstellung durchführen und die Ergebnisse abrufen. Dieser Ressourcentyp ist neu in ONTAP 9.8.

MetroCluster DR-Gruppen

Sie können Vorgänge für die MetroCluster DR-Gruppen durchführen. Dieser Ressourcentyp ist neu in ONTAP 9.8.

MetroCluster Interconnects

Sie können den MetroCluster-Verbindungsstatus abrufen. Dieser Ressourcentyp ist neu in ONTAP 9.8.

MetroCluster-Knoten

Sie können den Status der einzelnen Nodes in einer MetroCluster-Bereitstellung abrufen. Dieser Ressourcentyp ist neu in ONTAP 9.8.

MetroCluster Betrieb

Sie können eine Liste der kürzlich ausgeführten Vorgänge einer MetroCluster-Konfiguration abrufen. Dieser Ressourcentyp ist neu in ONTAP 9.8.

MetroCluster SVMs

Sie können Informationen zu allen SVM-Paaren in einer MetroCluster-Konfiguration abrufen. Dieser Ressourcentyp wurde mit ONTAP 9.11.1 eingeführt.

Knoten

ONTAP Cluster bestehen aus einem oder mehreren Nodes. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt und mit ONTAP 9.8 aktualisiert.

NTP-Schlüssel

Das Network Time Protocol (NTP) kann so konfiguriert werden, dass es freigegebene private Schlüssel zwischen ONTAP und vertrauenswürdigen externen NTP-Zeitservern verwendet. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

NTP-Server

Mit diesen API-Aufrufen können Sie die Einstellungen für das ONTAP-Netzwerkzeitprotokoll konfigurieren, einschließlich der externen NTP-Server und -Schlüssel. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

Kollegen

Die Peer-Objekte repräsentieren Endpunkte und unterstützen die Cluster-Peering-Beziehungen. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Performance-Zähler

Frühere ONTAP-Releases haben statistische Informationen über die betrieblichen Eigenschaften des Systems erhalten. In der Version 9.11.1 wurden die Informationen verbessert und sind nun über DIE REST API verfügbar. Diese Funktion bringt das ONTAP REST API näher an Parität mit dem Data ONTAP API (ONTAPI oder ZAPI). Dieser Ressourcentyp wurde mit ONTAP 9.11 eingeführt.

Ressourcen-Tags

Sie können Tags verwenden, um REST-API-Ressourcen zu gruppieren. Auf diese Weise können Sie verwandte Ressourcen innerhalb eines bestimmten Projekts oder einer bestimmten Organisationsgruppe zuordnen. Mithilfe von Tags können Sie Ressourcen effektiver organisieren und verfolgen. Dieser Ressourcentyp wurde mit ONTAP 9.13 eingeführt.

Zeitpläne

Zeitpläne können zur Automatisierung der Aufgabenstellungen genutzt werden. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Sensoren

Über diese Endpunkte können Sie Details zu allen Umgebungssensoren der Plattform abrufen. Dieser Ressourcentyp wurde mit ONTAP 9.11 eingeführt.

Software

Ein ONTAP Cluster umfasst das Cluster-Softwareprofil, die Erfassung von Softwarepaketen und die Erfassung

des Software-Verlaufs. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt und mit ONTAP 9.8 aktualisiert.

Web

Sie können diese Endpunkte verwenden, um die Webservices-Konfigurationen zu aktualisieren und die aktuelle Konfiguration abzurufen. Dieser Ressourcentyp wurde mit ONTAP 9.10 eingeführt.

Name Services

Sie können diese API-Aufrufe verwenden, um die von ONTAP unterstützten Namensdienste zu verwalten.

Cache

ONTAP Name Services unterstützt Caching zur Verbesserung von Performance und Resiliency. Die Konfiguration des Cache für Namensdienste kann nun über die REST-API abgerufen werden. Die Einstellungen können auf mehreren Ebenen angewendet werden, darunter Hosts, unix-Benutzer, unix-Gruppen und Netgroups. Dieser Ressourcentyp wurde mit ONTAP 9.11 eingeführt.

DDNS

Sie können die DDNS-Informationen (Dynamic DNS) anzeigen und das DDNS-Subsystem verwalten. Dieser Ressourcentyp ist neu in ONTAP 9.8.

DNS

DNS unterstützt die Integration des ONTAP-Clusters in Ihr Netzwerk. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt und mit ONTAP 9.13 erweitert.

Host-Datensatz

Mit diesen Endpunkten können Sie die IP-Adresse eines angegebenen Host-Namens sowie den Hostnamen für eine IP-Adresse anzeigen. Dieser Ressourcentyp wurde mit ONTAP 9.10 eingeführt.

LDAP

LDAP-Server können zur Verwaltung von Benutzerinformationen verwendet werden. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

LDAP-Schemata

Sie können die von ONTAP verwendeten LDAP-Schemata erstellen, ändern und auflisten. Es sind vier Standardschemata enthalten. Dieser Ressourcentyp wurde mit ONTAP 9.11 eingeführt.

Lokale Hosts

Mithilfe dieser Endpunkte können Sie die lokalen Zuordnungen für Hostnamen anzeigen und verwalten. Dieser Ressourcentyp wurde mit ONTAP 9.10 eingeführt.

Namenszuordnungen

Namenszuordnungen ermöglichen es Ihnen, Identitäten von einer Namensdomäne zu einer anderen zuzuordnen. Sie können beispielsweise Identitäten von CIFS zu UNIX, Kerberos zu UNIX und UNIX zu CIFS zuordnen. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Netzwerkgruppendateien

Sie können die Details zu den Netzwerkgruppen abrufen und eine Datei für eine SVM löschen. Dieser Ressourcentyp wurde mit ONTAP 9.11 eingeführt.

NIS

NIS-Server können zur Authentifizierung von Benutzern und Client-Workstations verwendet werden. Dieser

Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

UNIX-Benutzer und -Gruppen

Lokale UNIX-Benutzer und -Gruppen waren bereits Teil früherer ONTAP Versionen. Jetzt wurde der REST-API jedoch Unterstützung hinzugefügt, mit der Sie die Benutzer und Gruppen anzeigen und verwalten können. Diese REST-Ressourcentypen wurden mit ONTAP 9.9 eingeführt und in ONTAP 9.10 deutlich verbessert.

NAS

Mithilfe dieser API-Aufrufe können Sie die CIFS- und NFS-Einstellungen für den Cluster und die SVMs verwalten.

Active Directory

Sie können die für ein ONTAP-Cluster definierten Active Directory-Konten verwalten. Dies umfasst das Erstellen neuer Konten sowie das Anzeigen, Aktualisieren und Löschen von Konten. Diese Unterstützung wurde in ONTAP 9.12 hinzugefügt.

Prüfung

Bestimmte CIFS- und NFS-Ereignisse können für die SVMs protokolliert werden, um die Sicherheit zu verbessern. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Umleitung des Prüfprotokolls

Sie können NAS-Auditing-Ereignisse zu einer bestimmten SVM umleiten. Dieser Ressourcentyp ist neu in ONTAP 9.8.

CIFS-Verbindungen

Sie können eine Liste der festgelegten CIFS-Verbindungen abrufen. Dieser Ressourcentyp wurde mit ONTAP 9.11.1 eingeführt.

CIFS-Domänen

Auf Cluster- und SVM-Ebene mit verschiedenen Kategorien von Endpunkten wurde Unterstützung für CIFS-Domänen hinzugefügt. Sie können die Domänenkonfiguration abrufen sowie bevorzugte Domänen-Controller erstellen und entfernen. Dieser Ressourcentyp wurde mit ONTAP 9.10 eingeführt und mit ONTAP 9.13 erweitert.

CIFS-Gruppenrichtlinien

Endpunkte wurden hinzugefügt, um die Erstellung und das Management von CIFS-Gruppenrichtlinien zu unterstützen. Die Konfigurationsinformationen sind verfügbar und über Gruppenrichtlinienobjekte verwaltet, die auf alle oder bestimmte SVMs angewendet werden. Diese Unterstützung wurde in ONTAP 9.12 hinzugefügt.

Suchpfade für CIFS Home Directorys

Home Directories für SMB-Benutzer auf einem CIFS-Server können erstellt werden, ohne dass jeder Benutzer eine individuelle SMB-Freigabe erstellt. Der Suchpfad für das Home Directory ist eine Gruppe von absoluten Pfaden aus dem Root einer SVM. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Lokale CIFS-Gruppen

Der CIFS-Server kann lokale Gruppen zur Autorisierung bei der Festlegung von Zugriffsrechten für Freigabe, Datei und Verzeichnis verwenden. Dieser Ressourcentyp wurde mit ONTAP 9.9 eingeführt und mit ONTAP 9.10 deutlich erweitert.

CIFS NetBIOS

Sie können Informationen zu den NetBIOS-Verbindungen für das Cluster anzeigen. Zu den Details gehören die

IP-Adressen und registrierte NetBIOS-Namen. Diese Informationen können Ihnen bei der Behebung von Problemen mit der Namensauflösung helfen. Dieser Ressourcentyp wurde mit ONTAP 9.11.1 eingeführt.

CIFS-Services

Die Kernkonfiguration des CIFS-Servers. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt und mit ONTAP 9.7 und 9.15 aktualisiert.

CIFS-Sitzungsdateien

Sie können eine Liste der offenen Dateien für die CIFS-Sitzungen auf Grundlage verschiedener Filteroptionen abrufen. Dieser Ressourcentyp wurde mit ONTAP 9.11.1 eingeführt.

CIFS-Sitzungen

Mit dieser API können Sie detaillierte Informationen über eine CIFS-Sitzung abrufen. Dieser Ressourcentyp wurde mit der ONTAP 9.8 REST API eingeführt und mit ONTAP 9.9 erweitert.

CIFS-Schattenkopien

Microsoft Remote Volume Shadow Copy Services ist eine Erweiterung der vorhandenen Microsoft VSS-Funktionalität. VSS wird erweitert, um Schatten-Kopien von SMB-Freigaben zu unterstützen. Diese Funktion ist jetzt über die ONTAP REST API verfügbar. Dieser Ressourcentyp wurde mit ONTAP 9.11.1 eingeführt.

CIFS-Freigaben

Die SMB-Freigaben werden auf einem CIFS-Server definiert. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

CIFS Shares ACLs

Die Zugriffssteuerungslisten (ACLs), die den Zugriff auf Ordner und Dateien auf den CIFS-Freigaben steuern. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

CIFS UNIX Symlink-Zuordnung

Sowohl CIFS- als auch UNIX-Clients können auf denselben Datenspeicher zugreifen. Wenn UNIX-Clients symbolische Links erstellen, verweisen diese Zuordnungen auf eine andere Datei oder einen Ordner, um die CIFS-Clients zu unterstützen. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Massenimport von CIFS-Benutzern und Gruppen

Sie können die neuen REST-API-Endpunkte verwenden, um einen Massenimport der lokalen CIFS-Benutzer, -Gruppen und -Gruppenmitglieddaten durchzuführen und den Status der Anforderung zu überwachen. Dieser Ressourcentyp wurde mit ONTAP 9.11.1 eingeführt.

Verfolgung des Dateizugriffs

Sie können diese API-Aufrufe verwenden, um den Zugriff auf bestimmte Dateien zu verfolgen. Dieser Ressourcentyp ist neu in ONTAP 9.8.

Dateisicherheitsberechtigungen

Sie können diese API-Aufrufe verwenden, zeigt die effektiven Berechtigungen an, die Windows- oder Unix-Benutzer für eine bestimmte Datei oder einen bestimmten Ordner gewährt haben. Sie können auch NTFS-Dateisicherheitsrichtlinien und Audit-Richtlinien verwalten. Dieser Ressourcentyp wurde mit der ONTAP 9.8 REST API eingeführt und wurde mit ONTAP 9.9 deutlich verbessert.

FPolicy

FPolicy ist ein Framework für Dateizugriffsbenachrichtigungen zur Überwachung und Verwaltung von Ereignissen, die Dateizugriffe auf den SVMs betreffen. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

FPolicy-Verbindungen

Mit diesen Endpunkten können Sie Verbindungsinformationen für externe FPolicy-Server anzeigen und aktualisieren. Dieser Ressourcentyp wurde mit ONTAP 9.10 eingeführt.

FPolicy-Engines

Die FPolicy-Engines ermöglichen es Ihnen, die externen Server zu identifizieren, die die Dateizugriffsbenachrichtigungen erhalten. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

FPolicy-Ereignisse

Die Konfiguration bestimmt, wie der Dateizugriff überwacht wird und welche Ereignisse generiert werden. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Persistenter FPolicy-Speicher

Sie können einen persistenten Speicher für die ONTAP FPolicy Konfiguration und Ereignisse konfigurieren und verwalten. Jede SVM kann über einen persistenten Speicher verfügen, der für mehrere Richtlinien in der SVM freigegeben wird. Dieser Ressourcentyp wurde mit ONTAP 9.14 eingeführt.

FPolicy-Richtlinien

Ein Container für Elemente des FPolicy Framework, einschließlich FPolicy-Engines und Ereignissen. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Verriegelt

Ein Sperrmechanismus ist ein Synchronisierungsmechanismus zur Durchsetzung von Beschränkungen für gleichzeitigen Zugriff auf Dateien, bei denen viele Clients gleichzeitig auf dieselbe Datei zugreifen. Sie können diese Endpunkte zum Abrufen und Löschen von Sperren verwenden. Dieser Ressourcentyp wurde mit ONTAP 9.10 eingeführt.

NFS Connected Client Maps

Die NFS-Map-Informationen für die verbundenen Clients stehen über den neuen Endpunkt zur Verfügung. Sie können Details zu dem Node, der SVM und der IP-Adresse abrufen. Dieser Ressourcentyp wurde mit ONTAP 9.11.1 eingeführt.

NFS-verbundene Clients

Sie können eine Liste der verbundenen Clients mit den Details ihrer Verbindung anzeigen. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

NFS-Exportrichtlinien

Richtlinien einschließlich Regeln, die die NFS-Exporte beschreiben Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

NFS Kerberos Schnittstellen

Die Konfigurationseinstellungen für eine Schnittstelle zu Kerberos. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

NFS Kerberos Bereiche

Die Konfigurationseinstellungen für Kerberos-Bereiche. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

NFS über TLS

Mit dieser Ressource können Sie die Schnittstellenkonfiguration abrufen und aktualisieren, wenn Sie NFS über TLS verwenden. Dieser Ressourcentyp wurde mit ONTAP 9.15 eingeführt.

NFS-Services

Die Kernkonfiguration des NFS-Servers. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt und mit ONTAP 9.7 aktualisiert.

Objektspeicher

Das Auditing von S3-Ereignissen ist eine Verbesserung der Sicherheit, die es ermöglicht, bestimmte S3-Ereignisse zu verfolgen und zu protokollieren. Ein S3-Audit-Ereigniswähler kann auf Bucket-Basis pro SVM festgelegt werden. Dieser Ressourcentyp wurde mit ONTAP 9.10 eingeführt.

Vscan

Eine Sicherheitsfunktion zum Schutz Ihrer Daten vor Viren und anderen schädlichen Codes. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Vscan-Zugriffsrichtlinien

Die Vscan-Richtlinien, mit denen Dateiobjekte aktiv gescannt werden können, wenn ein Client darauf zugreift. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Vscan-On-Demand-Richtlinien

Die Vscan-Richtlinien ermöglichen das sofortige Scannen von Dateiobjekten nach Bedarf oder nach einem festgelegten Zeitplan. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Vscan-Scannerpools

Eine Reihe von Attributen, mit denen die Verbindung zwischen ONTAP und einem externen Virus-Scan-Server verwaltet wird. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Vscan-Serverstatus

Der Status des externen Virus-Scan-Servers. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

NDMP

Sie können diese API-Aufrufe zur Verwaltung der NDMP-Services verwenden.

NDMP-Modus

Der NDMP-Betriebsmodus kann vom Umfang der SVM oder vom Node festgelegt werden. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

NDMP-Knoten

Sie können die NDMP-Konfiguration der Nodes verwalten. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

NDMP-Sitzungen

Sie können NDMP-Sitzungsdetails für eine bestimmte SVM oder einen bestimmten Node abrufen und löschen. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

NDMP SVMs

Sie können die NDMP-Konfiguration der SVMs managen. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

Passwörter für NDMP SVM

Sie können innerhalb der SVM-Inhalte Passwörter für einen bestimmten NDMP-Benutzer generieren und abrufen. Dieser Ressourcentyp wurde mit der ONTAP 9.8 REST API eingeführt und mit ONTAP 9.9 erweitert.

Netzwerkbetrieb

Mithilfe dieser API-Aufrufe können Sie die physischen und logischen Netzwerkressourcen verwalten, die mit dem Cluster verwendet werden.

BGP-Peer-Gruppen

Sie können Peer-Gruppen für das Border Gateway Protocol erstellen und verwalten. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

Ethernet Broadcast-Domänen

Eine Ethernet Broadcast-Domäne ist ein Satz physischer Ports, die als Teil desselben physischen Netzwerks angezeigt werden. Alle Ports empfangen ein Paket, wenn sie von einem der Ports in der Domäne gesendet werden. Jede Broadcast-Domäne ist Teil eines IPspaces. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Ethernet-Ports

Ein Ethernet-Port ist ein physischer oder virtueller Netzwerkendpunkt. Die Ports können in einer Link Aggregate Group (LAG) oder mit einem Virtual LAN (VLAN) getrennt werden. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt und mit ONTAP 9.8 aktualisiert.

Ethernet-Switch-Ports

Sie können die Portinformationen für einen Ethernet-Switch abrufen. Dieser Ressourcentyp ist neu in ONTAP 9.8.

Ethernet-Switches

Sie können die Konfiguration für Ethernet-Switches abrufen oder ändern, die für das ONTAP-Cluster oder das Storage-Netzwerk verwendet werden. Dieser Ressourcentyp ist neu in ONTAP 9.8 und aktualisiert mit 9.11.

Fibre Channel Fabrics

Informationen über das FC-Netzwerk können über die REST-API-Endpunkte der Fibre Channel (FC)-Fabric abgerufen werden. Dazu gehören auch die Verbindungen zwischen dem ONTAP-Cluster und der FC-Fabric, die Switches aus der Fabric und die Zonen des aktiven zoneset. Dieser Ressourcentyp wurde mit ONTAP 9.11 eingeführt.

Fibre Channel-Schnittstellen

Eine Fibre-Channel-Schnittstelle ist ein logischer Endpunkt einer SVM. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt und mit ONTAP 9.8 aktualisiert. Die Unterstützung für das Abrufen von Performance-Kennzahlen-Daten wurde mit ONTAP 9.14 hinzugefügt.

Fibre-Channel-Ports

Ein Fibre Channel-Port ist ein physischer Adapter auf einem ONTAP-Node, der zur Verbindung mit dem Fibre Channel-Netzwerk verwendet wird. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt und mit ONTAP 9.8 aktualisiert. Die Unterstützung für das Abrufen von Performance-Kennzahlen-Daten wurde mit ONTAP 9.14 hinzugefügt.

HTTP-Proxy

Sie können einen HTTP-Proxy für eine SVM oder einen Cluster-IPSpace konfigurieren. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

IP-Schnittstellen

Eine logische Schnittstelle (LIF) ist eine IP-Adresse mit zusätzlichen Konfigurationsattributen. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt und mit ONTAP 9.8 aktualisiert.

IP-Routen

Eine Routing-Tabelle ist eine Sammlung von IP-Routen, die zur Weiterleitung des Datenverkehrs an sein Ziel verwendet werden. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

IP-Service-Richtlinien

Die IP-Service-Richtlinien definieren die Services, die in einem bestimmten LIF verfügbar sind. Service-Richtlinien können im Kontext einer SVM oder eines IPspace konfiguriert werden. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt und mit ONTAP 9.8 aktualisiert.

IP-Subnetze

Die ONTAP-Netzwerkfunktion wurde erweitert und unterstützt IP-Subnetze. Die REST-API bietet Zugriff auf die Konfiguration und das Management der IP-Subnetze innerhalb eines ONTAP-Clusters. Dieser Ressourcentyp wurde mit ONTAP 9.11 eingeführt.

IPspaces

Ein IPspace erstellt einen Netzwerkbereich, der eine oder mehrere SVMs unterstützt. Die IPspaces können voneinander isoliert werden, wodurch Sicherheit und Datenschutz gewährleistet sind. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

NVMe

Sie können diese API-Aufrufe verwenden, um Ressourcen zu verwalten, die NVMe (Non-Volatile Memory Express) unterstützen.

Fibre Channel-Anmeldungen

Die Fibre Channel-Logins stellen Verbindungen dar, die von Fibre Channel-Initiatoren gebildet wurden, die bei ONTAP angemeldet sind. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Namespaces

Ein NVMe Namespace ist eine Sammlung adressierbarer logischer Blöcke, die Hosts verwendet werden, die über das NVMe over Fabrics-Protokoll mit der SVM verbunden sind. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt und mit ONTAP 9.8 aktualisiert. Die Unterstützung für das Abrufen von Performance-Kennzahlen-Daten wurde mit ONTAP 9.14 hinzugefügt.

NVMe-Schnittstellen

NVMe-Schnittstellen sind die Netzwerkschnittstellen, die für die Unterstützung des NVMe over Fabrics-Protokolls (NVMe-of) konfiguriert sind. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

NVMe-Services

Ein NVMe-Service definiert die Eigenschaften des NVMe-Controller-Ziels für eine SVM. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt und mit ONTAP 9.7 aktualisiert. Die Unterstützung für das Abrufen von Performance-Kennzahlen-Daten wurde mit ONTAP 9.14 hinzugefügt.

NVMe-Subsystem-Controller

Die NVMe-Subsystem-Controller stellen dynamische Verbindungen zwischen Hosts und einer Storage-Lösung dar. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

NVMe-Subsystem-Zuordnungen

Eine NVMe-Subsystemzuordnung ist eine Zuordnung eines NVMe Namespace zu einem NVMe-Subsystem. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

NVMe-Subsysteme

Ein NVMe-Subsystem behält bei einer Konfiguration und bei der Namespace-Zugriffssteuerung für einen Satz NVMe-verbundenen Hosts die Kontrolle. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Objektspeicher

Über diese API-Aufrufe können Sie auf S3-basierten Objekt-Storage zugreifen.

Buckets

Ein Bucket ist ein Container von Objekten und ist unter Verwendung eines Objektnamens-Speicherplatzes strukturiert. Jeder S3-Objektserver kann über mehrere Buckets verfügen. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt und mit ONTAP 9.8 aktualisiert.

Services

Sie können die ONTAP S3-Konfiguration erstellen und managen, einschließlich Server- und Bucket-Konfigurationen. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

Service-Buckets

Ein Bucket ist ein Container von Objekten und ist unter Verwendung eines Objektnamens-Speicherplatzes strukturiert. Sie können die Buckets für einen bestimmten S3-Server managen. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

S3-Bucket-Regeln

Die S3-Buckets können eine Regeldefinition enthalten. Jede Regel ist ein Listenobjekt und definiert die Aktionen, die für ein Objekt innerhalb des Buckets ausgeführt werden sollen. Dieser Ressourcentyp wurde mit ONTAP 9.13 eingeführt.

S3-Gruppen

Sie können Gruppen von S3 Benutzern erstellen und die Zugriffssteuerung auf Gruppenebene managen. Dieser Ressourcentyp ist neu in ONTAP 9.8.

S3-Richtlinien

Sie können eine S3-Richtlinie erstellen und sie einer Ressource zuordnen, um verschiedene Berechtigungen zu definieren. Dieser Ressourcentyp ist neu in ONTAP 9.8.

Benutzer

Die S3-Benutzerkonten werden auf dem S3-Server verwaltet. Benutzerkonten basieren auf einem Schlüsselpaar und sind mit den von ihnen kontrollierter Buckets verknüpft. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

San

Sie können diese API-Aufrufe für das Management von SAN-Ressourcen (Storage Area Networking) verwenden.

Fibre Channel-Anmeldungen

Fibre Channel-Anmeldungen stellen Verbindungen dar, die von Fibre Channel-Initiatoren gebildet wurden, die bei ONTAP angemeldet sind. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Fibre Channel Protocol Services

Ein Fibre Channel Protocol (FCP)-Service definiert die Eigenschaften eines Fibre Channel-Ziels für eine SVM. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt und mit ONTAP 9.7 aktualisiert. Die Unterstützung für

das Abrufen von Performance-Kennzahlen-Daten wurde mit ONTAP 9.14 hinzugefügt.

Fibre Channel WWPN-Aliase

Ein der World Wide Port Name (WWPN) ist ein 64-bit-Wert, der einen Fibre Channel-Port eindeutig identifiziert. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

igroups

Eine Initiatorgruppe ist eine Sammlung von Fibre Channel-WWPNs (World Wide Port Names) und iSCSI IQNs (qualifizierte Namen) und iSCSI EUIs (Extended Unique Identifier), die Host-Initiatoren identifizieren. Dieser Ressourcentyp wurde ursprünglich mit ONTAP 9.6 eingeführt.

Geschachtelte Initiatorgruppen ist eine neue Funktion von ONTAP 9.9. Zudem wurde die REST-API unterstützt. Dieser REST-Ressourcentyp wurde mit ONTAP 9.9 eingeführt.

Initiatoren

Ein Initiator ist ein Fibre Channel (FC) World Wide Port Name (WWPN), ein iSCSI Qualified Name (IQN) oder ein iSCSI EUI (Extended Unique Identifier), der einen Host-Endpunkt identifiziert. Sie können Initiatoren für das Cluster oder eine bestimmte SVM abrufen. Dieser Ressourcentyp wurde mit ONTAP 9.14 eingeführt.

ISCSI-Anmeldedaten

Das iSCSI-Anmeldeinformationen-Objekt enthält Authentifizierungsdaten, die von einem Initiator und ONTAP verwendet werden. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

ISCSI-Services

Ein iSCSI-Service definiert die Eigenschaften des iSCSI-Ziels für eine SVM. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt und mit ONTAP 9.7 aktualisiert. Die Unterstützung für das Abrufen von Performance-Kennzahlen-Daten wurde mit ONTAP 9.14 hinzugefügt.

ISCSI-Sitzungen

Eine iSCSI-Sitzung ist eine oder mehrere TCP-Verbindungen, die einen iSCSI-Initiator mit einem iSCSI-Ziel verbinden. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

LUN-Attribute

LUN-Attribute sind aufruferdefinierte Name-/Wertpaare, die optional mit einer LUN gespeichert werden können. Diese Attribute können zur Speicherung kleiner Mengen applikationsspezifischer Metadaten verwendet und werden nicht von ONTAP interpretiert. Mit den Endpunkten können Sie Attribute für eine LUN erstellen, aktualisieren, löschen und erkennen. Dieser Ressourcentyp wurde mit ONTAP 9.10 eingeführt.

LUN-Zuordnungen

Eine LUN-Zuordnung ist eine Zuordnung zwischen einer LUN und einer Initiatorgruppe. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

LUN ordnet den Knoten für die Berichterstellung zu

Die Knoten zur Berichterstellung sind die Cluster Nodes, von denen Netzwerkpfade zu einer zugeordneten LUN mithilfe der SAN-Protokolle als Teil der Selective LUN Map (SLM)-Funktion von ONTAP angekündigt werden. Mit den neuen Endpunkten können die Reporting-Nodes einer LUN-Zuordnung hinzugefügt, entfernt und ermittelt werden. Dieser Ressourcentyp wurde mit ONTAP 9.10 eingeführt.

LUNs

Eine LUN ist die logische Darstellung des Storage in einem Storage Area Network (SAN). Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt und mit ONTAP 9.7 aktualisiert. Die Unterstützung für das Abrufen von Performance-Kennzahlen-Daten wurde mit ONTAP 9.14 hinzugefügt.

Port-Sets

Ein Portsatz ist eine Sammlung von Fibre Channel- oder iSCSI-Netzwerkschnittstellen, die der Storage VM „*portset*“ zugeordnet sind. Während diese Funktion für frühere Versionen von ONTAP vorhanden war, wurde jetzt auch der REST API Support hinzugefügt. Dieser REST-Ressourcentyp wurde mit ONTAP 9.9 eingeführt.

VVol Bindungen

Ein VMware Virtual Volume (vVol) Bindung ist eine Verknüpfung zwischen einer LUN der Klasse `protocol_endpoint` Und eine LUN der Klasse `vvol`. Mit der vVol Binding REST API können Sie vVol Bindungen erstellen, löschen und entdecken. Dieser Ressourcentyp wurde mit ONTAP 9.10 eingeführt.

Sicherheit

Sie können diese API-Aufrufe verwenden, um die Sicherheitseinstellungen für das Cluster und SVM zu verwalten.

Konten

Es gibt eine Sammlung von Benutzerkonten für das Cluster und SVMs. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Kontobezeichnung

Konfiguration für ein Scoped-Benutzerkonto. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Active Directory-Proxy

Sie können die SVM-Kontoinformationen auf dem Active Directory-Server verwalten. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

Ransomware schützen

ONTAP erkennt Dateien, die möglicherweise eine Ransomware-Bedrohung enthalten. Es gibt mehrere Endgeräte-Kategorien. Sie können eine Liste dieser verdächtigen Dateien abrufen oder von einem Volume entfernen. Dieser Ressourcentyp wurde mit ONTAP 9.10.1 eingeführt.

Prüfung

Die Einstellungen, die bestimmen, was in den Audit-Log-Dateien protokolliert wird. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Audit-Ziele

Diese Einstellungen steuern, wie Audit-Log-Informationen an Remote-Systeme oder splunk Server übermittelt werden. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Audit-Meldungen

Sie können die Meldungen des Prüfprotokolls abrufen. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

AWS KMS

Amazon Web Services umfasst einen Verschlüsselungsmanagement-Service, der sicheren Storage für Schlüssel und andere Geheimnisse bietet. Sie können über die REST-API auf diesen Service zugreifen, sodass ONTAP seine Schlüssel sicher in der Cloud speichern kann. Darüber hinaus können Sie die mit NetApp Storage Encryption verwendeten Authentifizierungsschlüssel erstellen und auflisten. Diese Unterstützung ist in ONTAP 9.12 neu.

Azure Key Vault

Bei diesem Satz von API-Aufrufen können Sie Azure Schlüsselspeicher verwenden, um die ONTAP-Verschlüsselungsschlüssel zu speichern. Dieser Ressourcentyp ist neu in ONTAP 9.8.

Zertifikate

Mit den API-Aufrufen können von ONTAP verwendete Zertifikate installiert, angezeigt und gelöscht werden. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

Cisco Duo

Duo bietet zwei-Faktor-Authentifizierung für SSH-Anmeldungen. Sie können Duo für den Betrieb auf ONTAP-Cluster- oder SVM-Ebene konfigurieren. Dieser Ressourcentyp wurde mit ONTAP 9.14 eingeführt.

Cluster-Sicherheit

Sie können Details zur Cluster-weiten Sicherheit abrufen und bestimmte Parameter aktualisieren. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt und mit ONTAP 9.8 aktualisiert.

GCP-KMS

Mit diesem Satz von API-Aufrufen können Sie den Google Cloud Platform Key Management Service zum Speichern und Verwalten der ONTAP-Verschlüsselungsschlüssel verwenden. Dieser Ressourcentyp wurde zunächst mit der ONTAP 9.8 REST-API eingeführt. Diese Funktion wurde jedoch neu gestaltet und gilt bei neuen Ressourcentypen in ONTAP 9.9 als neu.

IPsec

Internet Protocol Security (IPSec) ist eine Protokollsuite, die Sicherheit zwischen zwei Endpunkten über ein zugrunde liegendes IP-Netzwerk bietet. Dieser Ressourcentyp ist neu in ONTAP 9.8.

IPsec CA-Zertifikate

Sie können IPSec-CA-Zertifikate hinzufügen, entfernen und abrufen. Dieser Ressourcentyp ist neu in ONTAP 9.10.

IPsec-Richtlinien

Mit diesem Satz von API-Aufrufen können Sie die für eine IPSec-Bereitstellung geltenden Richtlinien verwalten. Dieser Ressourcentyp ist neu in ONTAP 9.8.

IPsec-Sicherheitszuordnungen

Sie können diesen Satz von API-Aufrufen verwenden, um die für eine IPSec-Bereitstellung relevanten Sicherheitszuordnungen zu verwalten. Dieser Ressourcentyp ist neu in ONTAP 9.8.

Konfiguration für Schlüsselmanager

Mit diesen Endpunkten können Sie die Konfigurationen für Schlüsselmanager abrufen und aktualisieren. Dieser Ressourcentyp ist neu in ONTAP 9.10.

Schlüsselmanager

Ein Schlüsselmanager erlaubt Client-Modulen innerhalb von ONTAP, sicher gespeicherte Schlüssel zu speichern. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt und für ONTAP 9.7 aktualisiert. Ein weiteres Update mit ONTAP 9.12 zur Unterstützung der Authentifizierungsschlüssel war vorhanden. In ONTAP 9.13 wurde eine Wiederherstellungsfunktion hinzugefügt.

Schlüsselspeicher

Ein Schlüsselspeicher beschreibt den Typ eines Schlüsselmanagers. Dieser Ressourcentyp ist neu in ONTAP 9.10. Weitere Endpunkte, die eine verbesserte Steuerung unterstützen, wurden mit ONTAP 9.14 hinzugefügt.

LDAP-Authentifizierung

Diese API-Aufrufe werden zum Abrufen und Verwalten der Cluster-LDAP-Serverkonfiguration verwendet. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Anmeldungsmeldungen

Wird zum Anzeigen und Verwalten der von ONTAP verwendeten Login-Meldungen verwendet. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Verifizierung mehrerer Administratoren

Die Überprüfungsfunktion für mehrere Administratoren stellt ein flexibles Autorisierungs-Framework zum Schutz des Zugriffs auf ONTAP-Befehle oder -Vorgänge bereit. Es gibt 17 neue Endpunkte, die das Definieren, anfordern und Genehmigen von Zugriff in den folgenden Bereichen unterstützen:

- Regeln
- Anträge
- Genehmigungsgruppen

Wenn mehrere Administratoren Zugriff genehmigen können, lässt sich die Sicherheit Ihrer ONTAP- und IT-Umgebungen verbessern. Diese Ressourcentypen wurden mit ONTAP 9.11 eingeführt.

NIS-Authentifizierung

Diese Einstellungen werden zum Abrufen und Verwalten der NIS-Serverkonfiguration des Clusters verwendet. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

OAuth 2.0

Open Authorization (OAuth 2.0) ist ein Token-basiertes Framework, mit dem der Zugriff auf Ihre ONTAP Storage-Ressourcen eingeschränkt werden kann. Sie können sie zusammen mit Clients verwenden, die über die REST-API auf ONTAP zugreifen. Die Konfiguration kann mit jeder der ONTAP-Administrationsschnittstellen, einschließlich der REST-API, durchgeführt werden. Dieser Ressourcentyp wurde mit ONTAP 9.14 eingeführt.

Passwortrauthentifizierung

Dazu gehört auch der API-Aufruf, der zum Ändern des Kennworts eines Benutzerkontos verwendet wird. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Berechtigungen für eine Rolleninstanz

Verwalten Sie die Berechtigungen für eine bestimmte Rolle. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Authentifizierung über öffentlichen Schlüssel

Sie können diese API-Aufrufe verwenden, um die öffentlichen Schlüssel für Benutzerkonten zu konfigurieren. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

Rollen

Die Rollen bieten eine Möglichkeit, Benutzerkonten Berechtigungen zuzuweisen. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Instanz Rollen

Spezifische Instanz einer Rolle. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

SAML-Service-Provider

Sie können die Konfiguration für den SAML-Dienstanbieter anzeigen und verwalten. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

SSH

Mit diesen Aufrufen können Sie die SSH-Konfiguration festlegen. Dieser Ressourcentyp wurde mit ONTAP 9.7

eingeführt.

SSH SVMs

Mit diesen Endpunkten können Sie die SSH-Sicherheitskonfiguration für alle SVMs abrufen. Dieser Ressourcentyp wurde mit ONTAP 9.10 eingeführt.

TOTPS

Sie können die REST-API verwenden, um zeitbasierte TOTP-Profile (One-Time Password) für Konten zu konfigurieren, die sich über SSH anmelden und auf ONTAP zugreifen. Dieser Ressourcentyp wurde mit ONTAP 9.13 eingeführt.

SnapLock

Sie können diese API-Aufrufe verwenden, um die ONTAP SnapLock-Funktion zu verwalten.

Protokoll

Die SnapLock-Protokollstruktur basiert auf Verzeichnissen und Dateien auf einem bestimmten Volume, das die Protokolldatensätze enthält. Log-Dateien werden entsprechend der maximalen Protokollgröße gefüllt und archiviert. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

Compliance-Uhr

Die Compliance-Uhr bestimmt die Ablaufzeit der SnapLock-Objekte. Die Uhr muss außerhalb der REST-API initialisiert werden und kann nicht geändert werden. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

Aufbewahrung von Ereignissen

Mit der Funktion „SnapLock Event Based Retention“ (EBR) können Sie festlegen, wie lange eine Datei nach dem Auftreten eines Ereignisses aufbewahrt wird. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

Aufbewahrung von Dateien und privilegiertes Löschen

Sie können die Aufbewahrungszeit einer Datei verwalten, die von SnapLock erstellt wurde. Bei Bedarf können Sie AUCH noch nicht abgelaufene WORM-Dateien auf einem SnapLock Enterprise Volume löschen. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

> Die einzige integrierte Rolle mit Berechtigung, den Löschvorgang auszuführen, ist vsadmin-snaplock.

Fingerabdruck für Dateien

Sie können die wesentlichen Informationen, die Dateien und Volumes beschreiben, anzeigen und managen, z. B. Typ und Ablaufdatum. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

Gesetzliche Aufbewahrungspflichten

Sie können diese API-Aufrufe verwenden, um Dateien zu verwalten, die Teil eines Prozesses sind. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

SnapMirror

Mit diesen API-Aufrufen können Sie die SnapMirror Datensicherungstechnologie managen.

Richtlinien

Die SnapMirror Richtlinien werden auf Beziehungen angewendet und steuern die Konfigurationsattribute und das Verhalten der einzelnen Beziehungen. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Beziehungen

Sowohl asynchrone als auch synchrone Beziehungen legen die Konnektivität fest, die Sie für die Datenübertragung benötigen. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Beziehungsübertragungen

Sie können SnapMirror Transfers über vorhandene SnapMirror Beziehungen verwalten. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Storage

Diese API-Aufrufe können Sie zum Management des physischen und logischen Storage verwenden.

Aggregieren von Kennzahlen

Sie können Verlaufsdaten für Metriken für ein bestimmtes Aggregat abrufen. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt und mit ONTAP 9.7 aktualisiert.

Aggregieren von Plexen

Eine physische Kopie des WAFL Storage innerhalb eines Aggregats. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Aggregate

Ein Aggregat besteht aus einer oder mehreren RAID-Gruppen. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Brücken

Sie können die Brücken in einem Cluster abrufen. Dieser Ressourcentyp wurde mit ONTAP 9.9 eingeführt.

Festplatten

Die physischen Laufwerke im Cluster. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt und mit ONTAP 9.7 und 9.8 aktualisiert.

Dateiklon

Mithilfe dieser Endpunkte können Dateiklone erstellt, der Split-Status abgerufen und Split-Lasten gemanagt werden. Die Endpunktressourcen für das Klonen von Dateien wurden erstmals mit ONTAP 9.6 eingeführt und mit ONTAP 9.8 erweitert. Mit ONTAP 9.10 wurden sie wieder deutlich ausgebaut.

Dateien werden verschoben

Über diese REST-API-Endpunkte können Dateien zwischen zwei FlexVol Volumes oder innerhalb eines FlexGroup Volume verschoben werden. Nachdem die Anfrage angenommen wurde, können Sie den Fortschritt und den Status überwachen. Dieser Ressourcentyp wurde mit ONTAP 9.11.1 eingeführt.

FlexCache

Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt und mit ONTAP 9.8 aktualisiert.

Ursprünge von FlexCache

FlexCache ist ein persistenter Cache eines Ursprungs-Volume. Dieser Ressourcentyp wurde ursprünglich mit ONTAP 9.6 eingeführt. Die Unterstützung wurde durch die ONTAP 9.9 REST API verbessert, um Änderungen über die HTTP-PATCH-Methode zu unterstützen.

Überwachte Dateien

Sie können bestimmte Dateien für zusätzliche Überwachung festlegen. Dieser Ressourcentyp ist neu in ONTAP 9.8.

Pools

Sie können einen gemeinsamen Speicherpool erstellen und die Speicherpools in einem Cluster abrufen. Dieser Ressourcentyp wurde mit ONTAP 9.11.1 eingeführt.

Ports

Storage-Ports des Clusters. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt und mit ONTAP 9.11.1 erweitert.

QOS-Richtlinien (QOS

Konfiguration von Richtlinien für die Servicequalität Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

QOS-Optionen

Mithilfe von Endpunkten können Sie QOS-Optionen für das Cluster abrufen und festlegen. Sie können beispielsweise einen Prozentsatz der verfügbaren Systemverarbeitungsressourcen für Hintergrundaufgaben reservieren. Dieser Ressourcentyp wurde mit ONTAP 9.14 eingeführt.

QOS-Workloads

EIN QOS-Workload ist ein Storage-Objekt, das DURCH QOS nachverfolgt wird. SIE können die QOS-Workflows abrufen. Dieser Ressourcentyp wurde mit ONTAP 9.10 eingeführt.

Qtrees

Sie können diese API-Aufrufe zur Verwaltung von qtrees verwenden, einem Typ von logisch geteiltem Dateisystem. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Kontingentberichte

Berichte über Quoten, eine Technik zur Einschränkung oder Verfolgung von Dateien oder Platznutzung. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Kontingentregeln

Die Regeln, die zur Durchsetzung der Kontingente verwendet werden. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt und mit ONTAP 9.7 aktualisiert.

Shelfs

Shelfs im Cluster. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Snapshot-Richtlinien

Snapshots werden basierend auf Richtlinien erstellt. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Snapshot Zeitpläne

Sie können die Snapshot-Zeitpläne steuern. Dieser Ressourcentyp wurde mit ONTAP 9.8 neu gestaltet.

Schalter

Sie können die Switches in einem Cluster abrufen. Dieser Ressourcentyp wurde mit ONTAP 9.9 eingeführt.

Tape-Geräte

Sie können die Bandgeräte in einem Cluster abrufen. Dieser Ressourcentyp wurde mit ONTAP 9.9 eingeführt.

Wichtige Kennzahlen

Mit den Endpunkten mit den obersten Kennzahlen können Sie Aktivitäten für ein Volumen bestimmen, das nach einer bestimmten Metrik gefiltert wird. Die Filterung kann auf der Grundlage von Clients, Verzeichnissen, Dateien und Benutzern erfolgen. Dieser Ressourcentyp wurde mit ONTAP 9.10 eingeführt.

Richtlinien für Volume-Effizienz

Mit diesen API-Aufrufen können Sie die Effizienz konfigurieren, die auf ein gesamtes Volume angewendet wird. Dieser Ressourcentyp ist neu in ONTAP 9.8.

Volumes

Logische Container werden verwendet, um Clients Daten bereitzustellen. Dieser Ressourcentyp wurde ursprünglich mit der ONTAP 9.6 REST-API eingeführt. Viele der mit der API verwendeten Parameterwerte wurden mit ONTAP 9.9 deutlich erweitert, einschließlich der im Bereich Speicherplatzmanagement verwendeten.

Volume-Dateien

Sie können eine Liste von Dateien und Verzeichnissen für ein bestimmtes Verzeichnis auf einem Volume abrufen. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt und mit ONTAP 9.8 aktualisiert.

Volumes Snapshots

Snapshots für ein Volume. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Unterstützung

Sie können diese API-Aufrufe verwenden, um die ONTAP-Funktionen zu verwalten, die zur Unterstützung eines Clusters verwendet werden.

Applikationsprotokoll

Eine eigenständige Anwendung kann EMS-Ereignisse und optional generierte AutoSupport-Pakete bei einem ONTAP-System durch Ausgabe einer POST-Anfrage aufzeichnen. Dieser Ressourcentyp wurde mit ONTAP 9.11.1 eingeführt

Automatische Aktualisierung

Mit der automatischen Aktualisierungsfunktion bleiben Ihre ONTAP-Systeme auf dem Laufenden, indem Sie die neuesten Software-Updates herunterladen und anwenden. Es gibt verschiedene Endpunktkategorien zur Unterstützung der Funktion, einschließlich Status, Konfiguration und Updates. Diese Ressourcentypen wurden mit ONTAP 9.10 eingeführt.

AutoSupport

AutoSupport sammelt Konfigurations- und Statusdetails sowie Fehler und meldet die Informationen an NetApp. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

AutoSupport Nachrichten

Jeder Node behält AutoSupport Meldungen, die generiert und abgerufen werden können. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Konfigurations-Backup

Mit diesen APIs können Sie die aktuellen Backup-Einstellungen abrufen und aktualisieren. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Backup-Vorgänge der Konfiguration

Sie können Backup-Dateien der Konfiguration erstellen, abrufen und löschen. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

Core Dump

Mithilfe dieser Endpunkte können Sie die von einem Cluster oder Node generierten Memory Core Dumps abrufen und verwalten. Dieser Ressourcentyp wurde mit ONTAP 9.10 eingeführt.

EMS

Das Event Management System (EMS) sammelt Ereignisse und sendet Benachrichtigungen an ein oder mehrere Ziele. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

EMS-Ziele

Die EMS-Ziele bestimmen, wie und wo Benachrichtigungen gesendet werden. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Instanz für EMS-Ziele

Eine EMS-Zielinstanz ist nach Typ und Standort definiert. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

EMS-Events

Dies ist eine Live-Sammlung von Systemereignissen für den Cluster. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

EMS-Filter

Die EMS-Filter identifizieren gemeinsam die Ereignisse, die eine zusätzliche Bearbeitung erfordern. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Instanz für EMS-Filter

Eine EMS-Filterinstanz ist eine Sammlung von Regeln, die auf die Ereignisse angewendet werden. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

EMS-Nachrichten

Bietet Zugriff auf den EMS-Ereigniskatalog. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

EMS-Rollenkonfiguration

Die EMS-Support-Funktion ermöglicht die Verwaltung von Rollen und die Konfiguration der Zugriffssteuerung, die den Rollen zugewiesen ist. Dies bietet die Möglichkeit, die Ereignisse und Meldungen basierend auf der Rollenkonfiguration zu begrenzen oder zu filtern. Dieser Ressourcentyp wurde mit ONTAP 9.13 eingeführt.

EMS-Regeln für Filterinstanz

Für eine bestimmte Instanz eines EMS-Filters kann eine Liste von Regeln verwaltet werden. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Beispiel für EMS-Regeln für Filterinstanz

Eine einzelne Regel für eine bestimmte Instanz eines EMS-Filters. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

SNMP

Sie können SNMP- und Trap-Vorgänge für das Cluster aktivieren und deaktivieren. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

SNMP-Trap-Host

Ein SNMP-Trap-Host ist ein System, das für den Empfang von SNMP-Traps von ONTAP konfiguriert ist. Sie können die Hosts abrufen und definieren. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

SNMP-Trap-Host-Instanz

Sie können bestimmte SNMP-Trap-Hosts verwalten. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

SNMP-Benutzer

Sie können SNMP-Benutzer definieren und verwalten. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

Instanz für SNMP-Benutzer

Sie können einen bestimmten SNMP-Benutzer verwalten, wobei die Engine-ID der administrativen SVM oder der Daten-SVM zugeordnet ist. Dieser Ressourcentyp wurde mit ONTAP 9.7 eingeführt.

SVM

Sie können diese API-Aufrufe zum Managen von Storage Virtual Machines (SVMs) verwenden.

Migrationen

Sie können eine SVM von einem Quell-Cluster zu einem Ziel-Cluster migrieren. Die neuen Endpunkte bieten vollständige Kontrolle, einschließlich der Möglichkeit, den Migrationsvorgang anzuhalten, fortzusetzen, den Status abzurufen und einen Migrationsvorgang abzubrechen. Dieser Ressourcentyp wurde mit ONTAP 9.10 eingeführt.

Peer-Berechtigungen

Peer-Berechtigungen können zugewiesen werden, die die SVM-Peering-Beziehungen unterstützen. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Kollegen

Die Peering-Beziehungen etablieren die Konnektivität zwischen den SVMs. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

SVMs

Sie können die SVMs, die an einen Cluster gebunden sind, verwalten. Dieser Ressourcentyp wurde mit ONTAP 9.6 eingeführt.

Wichtige Kennzahlen

Sie können auf zusätzliche Performance-Kennzahlendaten für eine bestimmte SVM-Instanz zugreifen. Es sind vier Listen verfügbar, die jeweils die wichtigsten I/O-Aktivitäten für ONTAP FlexVol und FlexGroup Volumes enthalten. Die Listen umfassen:

- Clients
- Verzeichnisse
- Dateien
- Benutzer

Diese Ressourcentypen wurden mit ONTAP 9.11 eingeführt.

Web

Über diese Endpunkte können Sie die Sicherheitskonfiguration für Webservices für jede Daten-SVM aktualisieren und abrufen. Dieser Ressourcentyp wurde mit ONTAP 9.10 eingeführt.

Workflows

Die Nutzung der Workflows wird vorbereitet

Sie sollten sich mit der Struktur und dem Format der Workflows vertraut machen, bevor Sie sie bei einer Live-ONTAP-Implementierung verwenden.

Sie sollten sicherstellen, dass Ihre ONTAP-Version alle API-Aufrufe in den Workflows unterstützt, die Sie verwenden möchten. Siehe "API-Referenz" Finden Sie weitere Informationen.

Einführung

Ein *Workflow* ist eine Sequenz aus einem oder mehreren Schritten, die zum Erreichen einer bestimmten administrativen Aufgabe oder eines bestimmten Ziels erforderlich sind. Die ONTAP Workflows beinhalten die wichtigsten Schritte und Parameter, die Sie für jede Aufgabe benötigen. Sie dienen als Ausgangspunkt für die Anpassung Ihrer ONTAP Automatisierungsumgebung.

Schritttypen

Jeder Schritt in einem ONTAP Workflow besteht aus einem der folgenden Typen:

- REST-API-Aufruf (mit Details wie Curl- und JSON-Beispiele)
- Einen anderen ONTAP-Workflow ausführen oder aufrufen
- Verschiedene verwandte Aufgaben (z. B. eine Konfigurationsentscheidung)

REST-API-Aufrufe

Die meisten Workflow-Schritte sind REST-API-Aufrufe. Bei diesen Schritten wird ein gängiges Format verwendet, das ein Beispiel für eine Wellung und andere Informationen enthält. Siehe "API-Referenz" Weitere Informationen zu den REST-API-Aufrufen.

Workflows in einem Schritt

Ein Workflow kann nur einen Schritt enthalten. Diese *einstufigen Workflows* werden leicht anders formatiert als Workflows, die mehrere Schritte enthalten. Beispielsweise wird der explizite Schrittname entfernt. Die Aktion oder der Vorgang sollte aufgrund des Workflow-Titels eindeutig sein.

Eingabevariablen

Die Workflows sind so allgemein wie möglich ausgelegt, sodass sie in jeder ONTAP Umgebung eingesetzt werden können. Vor diesem Hintergrund verwenden die REST-API-Aufrufe Variablen in den Curl-Beispielen und andere Eingaben. Die REST-API-Aufrufe können dann problemlos an verschiedene ONTAP-Umgebungen angepasst werden.

Basis-URL-Format

Sie können die ONTAP-REST-API direkt über Curl oder eine Programmiersprache aufrufen. In diesem Fall unterscheidet sich die Basis-URL von der URL, die Sie für den Zugriff auf die ONTAP Online-Dokumentation oder den System Manager verwenden.

Wenn Sie direkt auf die API zugreifen, müssen Sie **API** an die Domain oder IP-Adresse anhängen. Beispiel:

`https://ontap.demo-example.com/api`

Siehe "So erhalten Sie Zugriff auf die ONTAP REST API" Finden Sie weitere Informationen.

Allgemeine Eingabeparameter

Es gibt mehrere Eingabeparameter, die häufig bei den meisten REST-API-Aufrufen verwendet werden. Diese Parameter werden in der Regel nicht in den einzelnen Workflows beschrieben. Sie sollten mit den Parametern vertraut sein. Siehe "Eingabevariablen, die eine API-Anforderung steuern" Finden Sie weitere Informationen.

Wenn für einen bestimmten REST API-Aufruf zusätzliche Parameter benötigt werden, sind diese im Abschnitt **zusätzliche Eingabeparameter für das Curl-Beispiel** für jeden Workflow enthalten.

Variablenformat

Die ID-Werte und andere Variablen, die mit den Workflow-Beispielen verwendet werden, sind undurchsichtig und können mit jedem ONTAP-Cluster variieren. Um die Lesbarkeit der Beispiele zu verbessern, werden keine Istwerte verwendet. Variablen werden stattdessen verwendet. Dieser Ansatz basiert auf einem konsistenten Format und einem Satz reservierter Namen und bietet mehrere Vorteile, darunter:

- Die Locken- und JSON-Proben sind besser lesbar und leichter zu verstehen.
- Da alle Schlüsselwörter das gleiche Format verwenden, können Sie sie schnell identifizieren.
- Es gibt keine Sicherheitsgefährdung, da die Werte nicht kopiert und wiederverwendet werden können.

Die Variablen sind so formatiert, dass sie in einer Bash Shell-Umgebung verwendet werden. Jede Variable beginnt mit einem Dollarzeichen und ist bei Bedarf in doppelte Anführungszeichen eingeschlossen. Dies macht sie für Bash erkennbar. Für die Namen wird immer Großbuchstaben verwendet.

Hier sind einige der häufigsten Variablen Schlüsselwörter. Diese Liste ist nicht erschöpfend und es werden bei Bedarf zusätzliche Variablen verwendet. Ihre Bedeutung sollte auf der Grundlage des Kontexts offensichtlich sein.

Stichwort	Typ	Beschreibung
FQDN_IP-DOLLAR	URL	Der vollständig qualifizierte Domain-Name oder die IP-Adresse der ONTAP Management LIF.
„CLUSTER_ID“	Pfad	Der UUIDv4-Wert, der den ONTAP-Cluster identifiziert, auf dem die API-Vorgänge ausgeführt werden.
BASIC_AUTH	Kopfzeile	Die Zeichenfolge für die Anmeldeinformationen, die für die grundlegende HTTP-Authentifizierung verwendet wird.

Beispiele für JSON-Eingaben

Einige REST-API-Aufrufe, z. B. die, die POST oder PATCH verwenden, erfordern JSON-Eingaben im Körper der Anforderung. Zur Übersichtlichkeit werden die JSON-Eingabebeispiele getrennt von den Curl-Beispielen dargestellt. Sie können die JSON-Eingabebeispiele mit einer der unten beschriebenen Techniken verwenden.

In lokale Datei speichern

Sie können das JSON-Eingabebeispiel in eine Datei kopieren und lokal speichern. Der Curl-Befehl bezieht sich auf die Datei, die den verwendet `--data` Parameter mit dem Wert, der den Dateinamen mit einem angibt `@` Präfix.

Fügen Sie sie nach dem Beispiel in die Klemme ein

Zuerst müssen Sie das Beispiel für die Wellung kopieren und in eine Klemmenschale einfügen. Bearbeiten Sie dann das Beispiel, um den vollständig zu entfernen `--data` Am Ende des Parameters und ersetzen Sie ihn durch `--data-raw` Parameter. Kopieren Sie schließlich das JSON-Beispiel, und fügen Sie es ein, so dass es dem Curl-Befehl mit dem aktualisierten Parameter folgt. Sie sollten einfache Anführungszeichen verwenden, um das JSON-Eingabebeispiel zu umschließen.

Authentifizierungsoptionen

Die primäre für die REST-API verfügbare Authentifizierungsmethode ist die HTTP-Basisauthentifizierung. Ab ONTAP 9.14 haben Sie zudem die Möglichkeit, das Open Authorization (OAuth 2.0)-Framework mit Token-basierter Authentifizierung und Autorisierung zu verwenden.

HTTP-Basisauthentifizierung

Bei der Verwendung der grundlegenden Authentifizierung müssen die Benutzeranmeldeinformationen in jede HTTP-Anforderung einbezogen werden. Es gibt zwei Optionen zum Senden der Anmeldeinformationen.

Erstellen Sie den HTTP-Anforderungsheader

Sie können den Autorisierungskopf manuell erstellen und in die HTTP-Anforderungen einbeziehen. Dies ist möglich, wenn Sie einen Curl-Befehl in der CLI oder eine Programmiersprache mit Ihrem Automatisierungscode verwenden. Zu den grundlegenden Schritten gehören:

1. Verketten Sie die Benutzer- und Kennwortwerte mit einem Doppelpunkt:

   ```
   admin:david123
   ```

2. Konvertieren Sie den gesamten String in base64:

   ```
   YWRtaW46ZGF2aWQxMjM=
   ```

3. Erstellen Sie den Anforderungskopf:

   ```
   Authorization: Basic YWRtaW46ZGF2aWQxMjM=
   ```

Die Workflow-Curl-Beispiele enthalten diesen Header mit der Variablen **€BASIC_AUTH**, die Sie vor der Verwendung aktualisieren müssen.

Verwenden Sie einen Curl-Parameter

Eine weitere Option bei der Verwendung von Curl ist, den Autorisierungskopf zu entfernen und stattdessen den Curl **user**-Parameter zu verwenden. Beispiel:

```
--user username:password
```

Sie müssen die entsprechenden Anmeldedaten für Ihre Umgebung ersetzen. Die Anmeldeinformationen sind in base64 nicht kodiert. Wenn Sie den Befehl curl mit diesem Parameter ausführen, wird der String codiert und der Autorisierungskopf für Sie generiert.

OAuth 2.0

Wenn Sie OAuth 2.0 verwenden, müssen Sie ein Zugriffstoken von einem externen Autorisierungsserver anfordern und diese bei jeder HTTP-Anforderung einschließen. Im Folgenden werden die grundlegenden übergeordneten Schritte beschrieben. Siehe auch "Überblick über die Implementierung von ONTAP OAuth 2.0"

Weitere Informationen zu OAuth 2.0 und zur Verwendung mit ONTAP.

Bereiten Sie Ihre ONTAP-Umgebung vor

Bevor Sie die REST-API für den Zugriff auf ONTAP verwenden, müssen Sie die ONTAP-Umgebung vorbereiten und konfigurieren. Im allgemeinen sind die Schritte:

- ONTAP geschützte Ressourcen und Clients ermitteln
- Prüfen Sie die vorhandene ONTAP-REST-Rolle und Benutzerdefinitionen
- Installieren und Konfigurieren des Autorisierungsservers
- Entwerfen und Konfigurieren der Client-Autorisierungsdefinitionen
- Konfigurieren Sie ONTAP, und aktivieren Sie OAuth 2.0

Fordern Sie ein Zugriffstoken an

Mit ONTAP und dem definierten und aktiven Autorisierungsserver können Sie einen REST-API-Aufruf mit einem OAuth 2.0-Token erstellen. Der erste Schritt besteht darin, ein Zugriffstoken vom Autorisierungsserver anzufordern. Dies geschieht außerhalb von ONTAP mit einer von mehreren verschiedenen Techniken auf der Grundlage des Servers. ONTAP gibt keine Zugriffstoken aus und führt keine Umleitung durch.

Erstellen Sie den HTTP-Anforderungsheader

Nachdem Sie ein Zugriffstoken erhalten haben, können Sie einen Autorisierungs-Header erstellen und ihn mit den HTTP-Anforderungen integrieren. Unabhängig davon, ob Sie Curl oder eine Programmiersprache für den Zugriff auf die REST-API verwenden, müssen Sie den Header bei jeder Client-Anforderung einschließen. Sie können die Kopfzeile wie folgt erstellen:

```
Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSld …
```

Verwenden der Beispiele mit Bash

Wenn Sie die Workflow-Curl-Beispiele direkt verwenden, müssen Sie die darin enthaltenen Variablen mit Werten aktualisieren, die für Ihre Umgebung geeignet sind. Sie können die Beispiele manuell bearbeiten oder sich darauf verlassen, dass die Bash-Shell die Ersetzung für Sie wie unten beschrieben durchsetzt.

Ein Vorteil der Verwendung von Bash ist, dass Sie die Variablenwerte einmal in einer Shell-Sitzung anstatt einmal pro Curl-Befehl einstellen können.

Schritte

1. Öffnen Sie die Bash Shell, die mit Linux oder einem ähnlichen Betriebssystem geliefert wird.
2. Legen Sie die Variablenwerte fest, die in dem zu laufenden Curl-Beispiel enthalten sind. Beispiel:

   ```
   CLUSTER_ID=ce559b75-4145-11ee-b51a-005056aee9fb
   ```

3. Kopieren Sie das Beispiel für die Wellung von der Workflow-Seite, und fügen Sie es in das Shell-Terminal ein.
4. Drücken Sie **ENTER**, um Folgendes zu tun:
   a. Ersetzen Sie die von Ihnen festgelegten Variablenwerte
   b. Führen Sie den Befehl curl aus

Cluster

Get Cluster-Konfiguration

Sie können die Konfiguration für ein ONTAP Cluster einschließlich bestimmter Felder abrufen. Dies kann im Rahmen der Bewertung des Status des Clusters oder vor dem Aktualisieren der Konfiguration erfolgen.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
GET	/API/Cluster

Zusätzliche Eingabeparameter für Curl-Beispiele

Neben den bei allen REST API-Aufrufen üblichen Parametern werden in diesem Schritt auch die folgenden Parameter im Curl-Beispiel verwendet.

Parameter	Typ	Erforderlich	Beschreibung
Felder	Abfrage	Nein	Wählen Sie die Werte aus, die zurückgegeben werden sollen. Beispiele `contact` Und `version`.

Curl Beispiel: Rufen Sie die Kontaktinformationen des Clusters ab

Dieses Beispiel zeigt, wie ein einzelnes Feld abgerufen wird. Um das gesamte Cluster-Objekt und die Konfiguration anzuzeigen, müssen Sie den entfernen `fields` Abfrageparameter.

```
curl --request GET \
--location "https://$FQDN_IP/api/cluster?fields=contact" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Beispiel für eine JSON-Ausgabe

```
{
  "contact": "support@company-demo.com"
}
```

Cluster-Kontakt aktualisieren

Sie können die Kontaktinformationen für ein Cluster aktualisieren. Da die Anforderung asynchron verarbeitet wird, müssen Sie auch feststellen, ob der zugehörige Hintergrundjob erfolgreich abgeschlossen wurde.

Schritt: Aktualisieren Sie die Kontaktinformationen des Clusters

Sie können einen API-Aufruf ausgeben, um die Kontaktinformationen des Clusters zu aktualisieren.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
PATCH	/API/Cluster

Verarbeitungsart

Asynchron

Beispiel für die Wellung

```
curl --request PATCH \
--location "https://$FQDN_IP/api/cluster" \
--include \
--header "Content-Type: application/json" \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON-Eingabebeispiel

```
{
  "contact": "support@company-demo.com"
}
```

Beispiel für eine JSON-Ausgabe

Ein Jobobjekt wird zurückgegeben. Sie sollten die Jobkennung speichern, um sie im nächsten Schritt zu verwenden.

```
{ "job": {
    "uuid": "d877f5bb-3aa7-11e9-b6c6-005056a78c89",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/d877f5bb-3aa7-11e9-b6c6-005056a78c89"
      }
    }
  }
}
```

Schritt 2: Rufen Sie den Status des Jobs ab

Führen Sie den Workflow aus "Job-Instanz abrufen" Und bestätigen Sie die `state` Wert ist `success`.

Schritt 3: Bestätigen Sie die Kontaktinformationen zum Cluster

Führen Sie den Workflow aus "Get Cluster-Konfiguration". Sie sollten die einstellen `fields` Abfrageparameter an `contact`.

Job-Instanz abrufen

Sie können die Instanz eines bestimmten ONTAP-Jobs abrufen. In der Regel möchten Sie feststellen, ob der Job und der zugehörige Vorgang erfolgreich abgeschlossen wurden.

Sie benötigen die UUID des Jobobjekts, die normalerweise nach der Ausgabe einer asynchronen Anforderung bereitgestellt wird. Überprüfen Sie auch "Asynchrone Verarbeitung mit dem Job-Objekt" Vor der Arbeit mit internen ONTAP Jobs.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
GET	/API/Cluster/Jobs/{uUID}

Verarbeitungsart

Synchron

Zusätzliche Eingabeparameter für die Curl-Beispiele

Zusätzlich zu den Parametern, die bei allen REST-API-Aufrufen üblich sind, werden die folgenden Parameter auch in den Curl-Beispielen für diesen Schritt verwendet.

Parameter	Typ	Erforderlich	Beschreibung
US-DOLLAR JOB_ID	Pfad	Ja.	Erforderlich, um den angeforderten Job zu identifizieren.

Beispiel für die Wellung

```
curl --request GET \
--location "https://$FQDN_IP/api/cluster/jobs/$JOB_ID" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Beispiel für eine JSON-Ausgabe

Der Statuswert und andere Felder werden in das zurückgegebene Jobobjekt aufgenommen. Der Job in diesem Beispiel wurde im Rahmen der Aktualisierung eines ONTAP-Clusters ausgeführt.

```
{
  "uuid": "d877f5bb-3aa7-11e9-b6c6-005056a78c89",
  "description": "PATCH /api/cluster",
  "state": "success",
  "message": "success",
  "code": 0,
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/d877f5bb-3aa7-11e9-b6c6-005056a78c89"
    }
  }
}
```

NAS

Dateisicherheitsberechtigungen

Bereiten Sie sich auf das Management von Dateisicherheits- und Audit-Richtlinien vor

Sie können die Berechtigungen und Audit-Richtlinien für Dateien managen, die über die SVMs innerhalb eines ONTAP Clusters verfügbar sind.

Überblick

ONTAP weist Dateiobjekten mithilfe von System Access Control Lists (SACLs) und Ermessensary Access Control Lists (DACLs) Berechtigungen zu. Ab ONTAP 9.9 unterstützt die REST-API das Management der SACL- und DACL-Berechtigungen. Sie können die API verwenden, um die Administration der Dateisicherheitsberechtigungen zu automatisieren. In vielen Fällen können Sie einen einzelnen REST API-Aufruf anstelle mehrerer CLI-Befehle oder ONTAPI (ZAPI)-Aufrufe verwenden.

> Bei ONTAP-Versionen vor 9.9 können Sie die Verwaltung der SACL- und DACL-Berechtigungen mithilfe der CLI-Passthrough-Funktion automatisieren. Siehe "Überlegungen zur Migration" Und "Verwenden des privaten CLI-Passthrough mit der ONTAP REST API" Finden Sie weitere Informationen.

Es stehen verschiedene Beispiel-Workflows zur Verfügung, die veranschaulichen, wie Sie die ONTAP Dateisicherheitsdienste mithilfe der REST-API managen. Bevor Sie die Workflows verwenden und einen der REST-API-Aufrufe ausgeben, müssen Sie diese überprüfen "Die Nutzung der Workflows wird vorbereitet".

Wenn Sie Python verwenden, lesen Sie auch das Skript "file_security_permissions.py" Beispiele für die Automatisierung einiger Dateisicherheitsaktivitäten.

ONTAP REST API im Vergleich zu ONTAP-CLI-Befehlen

Bei vielen Aufgaben erfordert die Verwendung der ONTAP REST-API weniger Aufrufe als die entsprechenden ONTAP CLI-Befehle oder ONTAPI (ZAPI)-Aufrufe. Die folgende Tabelle enthält eine Liste der API-Aufrufe und die entsprechenden CLI-Befehle, die für jede Aufgabe erforderlich sind.

ONTAP REST API	CLI VON ONTAP
`GET /protocols/file-security/effective-permissions/`	`vserver security file-directory show-effective-permissions`
`POST /protocols/file-security/permissions/`	1. `vserver security file-directory ntfs create` 2. `vserver security file-directory ntfs dacl add` 3. `vserver security file-directory ntfs sacl add` 4. `vserver security file-directory policy create` 5. `vserver security file-directory policy task add` 6. `vserver security file-directory apply`
`PATCH /protocols/file-security/permissions/`	`vserver security file-directory ntfs modify`
`DELETE /protocols/file-security/permissions/`	1. `vserver security file-directory ntfs dacl remove` 2. `vserver security file-directory ntfs sacl remove`

Verwandte Informationen

- "Python-Skript zur Darstellung von Dateiberechtigungen"
- "Vereinfachtes Management von Dateisicherheitsberechtigungen mit ONTAP REST-APIs"
- "Verwenden des privaten CLI-Passthrough mit der ONTAP REST API"

Holen Sie sich die effektiven Berechtigungen für eine Datei

Sie können die aktuellen effektiven Berechtigungen für eine bestimmte Datei oder einen bestimmten Ordner abrufen.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
GET	/API/protocols/file-Security/effective-permissions/{svm.uuid}/} path{

Verarbeitungsart

Synchron

Zusätzliche Eingabeparameter für Curl-Beispiele

Neben den bei allen REST API-Aufrufen üblichen Parametern werden in diesem Schritt auch die folgenden Parameter im Curl-Beispiel verwendet.

Parameter	Typ	Erforderlich	Beschreibung
SVM_ID USD	Pfad	Ja.	Dies ist die UUID der SVM, die die Datei enthält.
PFAD FÜR DATEI	Pfad	Ja.	Dies ist der Pfad zur Datei oder zum Ordner.

Beispiel für die Wellung

```
curl --request GET \
--location "https://$FQDN_IP/api/protocols/file-security/effective-
permissions/$SVM_ID/$FILE_PATH" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Beispiel für eine JSON-Ausgabe


```
{
  "svm": {
    "uuid": "cf5f271a-1beb-11ea-8fad-005056bb645e",
    "name": "vs1"
  },
  "user": "administrator",
  "type": "windows",
  "path": "/",
  "share": {
    "path": "/"
  },
  "file_permission": [
    "read",
    "write",
    "append",
    "read_ea",
    "write_ea",
    "execute",
    "delete_child",
    "read_attributes",
    "write_attributes",
    "delete",
    "read_control",
    "write_dac",
    "write_owner",
    "synchronize",
    "system_security"
  ],
  "share_permission": [
    "read",
    "read_ea",
    "execute",
    "read_attributes",
    "read_control",
    "synchronize"
  ]
}
```


Rufen Sie die Auditinformationen für eine Datei ab

Sie können die Überwachungsinformationen für eine bestimmte Datei oder einen bestimmten Ordner abrufen.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
GET	/API/protocols/file-Security/permissions/{svm.uuid}/} path{

Verarbeitungsart

Synchron

Zusätzliche Eingabeparameter für Curl-Beispiele

Neben den bei allen REST API-Aufrufen üblichen Parametern werden in diesem Schritt auch die folgenden Parameter im Curl-Beispiel verwendet.

Parameter	Typ	Erforderlich	Beschreibung
SVM_ID USD	Pfad	Ja.	Dies ist die UUID der SVM, die die Datei enthält.
PFAD FÜR DATEI	Pfad	Ja.	Dies ist der Pfad zur Datei oder zum Ordner.

Beispiel für die Wellung

```
curl --request GET \
--location "https://$FQDN_IP/api/protocols/file-
security/permissions/$SVM_ID/$FILE_PATH" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Beispiel für eine JSON-Ausgabe


```
{
  "svm": {
    "uuid": "9479099d-5b9f-11eb-9c4e-0050568e8682",
    "name": "vs1"
  },
  "path": "/parent",
  "owner": "BUILTIN\\Administrators",
  "group": "BUILTIN\\Administrators",
  "control_flags": "0x8014",
  "acls": [
    {
      "user": "BUILTIN\\Administrators",
      "access": "access_allow",
      "apply_to": {
        "files": true,
        "sub_folders": true,
        "this_folder": true
      },
```

```
      "advanced_rights": {
        "append_data": true,
        "delete": true,
        "delete_child": true,
        "execute_file": true,
        "full_control": true,
        "read_attr": true,
        "read_data": true,
        "read_ea": true,
        "read_perm": true,
        "write_attr": true,
        "write_data": true,
        "write_ea": true,
        "write_owner": true,
        "synchronize": true,
        "write_perm": true
      },
      "access_control": "file_directory"
    },
    {
      "user": "BUILTIN\\Users",
      "access": "access_allow",
      "apply_to": {
        "files": true,
        "sub_folders": true,
        "this_folder": true
      },
      "advanced_rights": {
        "append_data": true,
        "delete": true,
        "delete_child": true,
        "execute_file": true,
        "full_control": true,
        "read_attr": true,
        "read_data": true,
        "read_ea": true,
        "read_perm": true,
        "write_attr": true,
        "write_data": true,
        "write_ea": true,
        "write_owner": true,
        "synchronize": true,
        "write_perm": true
      },
      "access_control": "file_directory"
    }
```

```
  ],
  "inode": 64,
  "security_style": "mixed",
  "effective_style": "ntfs",
  "dos_attributes": "10",
  "text_dos_attr": "----D---",
  "user_id": "0",
  "group_id": "0",
  "mode_bits": 777,
  "text_mode_bits": "rwxrwxrwx"
}
```

Neue Berechtigungen auf eine Datei anwenden

Sie können eine neue Sicherheitsbeschreibung auf eine bestimmte Datei oder einen bestimmten Ordner anwenden.

Schritt 1: Die neuen Berechtigungen anwenden

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
POST	/API/protocols/file-Security/permissions/{svm.uuid}/} path{

Verarbeitungsart

Asynchron

Zusätzliche Eingabeparameter für Curl-Beispiele

Neben den bei allen REST API-Aufrufen üblichen Parametern werden in diesem Schritt auch die folgenden Parameter im Curl-Beispiel verwendet.

Parameter	Typ	Erforderlich	Beschreibung
SVM_ID USD	Pfad	Ja.	Dies ist die UUID der SVM, die die Datei enthält.
PFAD FÜR DATEI	Pfad	Ja.	Dies ist der Pfad zur Datei oder zum Ordner.

Beispiel für die Wellung

```
curl --request POST --location "https://$FQDN_IP/api/protocols/file-
security/permissions/$SVM_ID/$FILE_PATH?return_timeout=0" --include
--header "Accept */*" --header "Authorization: Basic $BASIC_AUTH" --data
'{ \"acls\": [ { \"access\": \"access_allow\", \"advanced_rights\": {
\"append_data\": true, \"delete\": true, \"delete_child\": true,
\"execute_file\": true, \"full_control\": true, \"read_attr\": true,
\"read_data\": true, \"read_ea\": true, \"read_perm\": true,
\"write_attr\": true, \"write_data\": true, \"write_ea\": true,
\"write_owner\": true, \"write_perm\": true }, \"apply_to\": { \"files\":
true, \"sub_folders\": true, \"this_folder\": true }, \"user\":
\"administrator\" } ], \"control_flags\": \"32788\", \"group\": \"S-1-5-
21-2233347455-2266964949-1780268902-69700\", \"ignore_paths\": [
\"/parent/child2\" ], \"owner\": \"S-1-5-21-2233347455-2266964949-
1780268902-69304\", \"propagation_mode\": \"propagate\"}'
```

Beispiel für eine JSON-Ausgabe

```
{
  "job": {
    "uuid": "3015c294-5bbc-11eb-9c4e-0050568e8682",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/3015c294-5bbc-11eb-9c4e-0050568e8682"
      }
    }
  }
}
```

Schritt 2: Rufen Sie den Status des Jobs ab

Führen Sie den Workflow aus "Job-Instanz abrufen" Und bestätigen Sie die `state` Wert ist `success`.

Die Informationen zum Sicherheitsdeskriptor aktualisieren

Sie können eine bestimmte Sicherheitsbeschreibung auf eine bestimmte Datei oder einen bestimmten Ordner aktualisieren, einschließlich der primären Eigentümer-, Gruppen- oder Kontrollflags.

Schritt 1: Aktualisieren Sie die Sicherheitsbeschreibung

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
PATCH	/API/protocols/file-Security/permissions/{svm.uuid}/} path{

Verarbeitungsart

Asynchron

Zusätzliche Eingabeparameter für Curl-Beispiele

Neben den bei allen REST API-Aufrufen üblichen Parametern werden in diesem Schritt auch die folgenden Parameter im Curl-Beispiel verwendet.

Parameter	Typ	Erforderlich	Beschreibung
SVM_ID USD	Pfad	Ja.	Dies ist die UUID der SVM, die die Datei enthält.
PFAD FÜR DATEI	Pfad	Ja.	Dies ist der Pfad zur Datei oder zum Ordner.

Beispiel für die Wellung

```
curl --request POST --location "https://$FQDN_IP/api/protocols/file-
security/permissions/$SVM_ID/$FILE_PATH?return_timeout=0" --include
--header "Accept */*" --header "Authorization: Basic $BASIC_AUTH" --data
'{ \"control_flags\": \"32788\", \"group\": \"everyone\", \"owner\":
\"user1\"}'
```

Beispiel für eine JSON-Ausgabe

```
{
  "job": {
    "uuid": "6f89e612-5bbd-11eb-9c4e-0050568e8682",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/6f89e612-5bbd-11eb-9c4e-0050568e8682"
      }
    }
  }
}
```

Schritt 2: Rufen Sie den Status des Jobs ab

Führen Sie den Workflow aus "Job-Instanz abrufen" Und bestätigen Sie die `state` Wert ist `success`.

Löschen eines Zugriffskontrolleintrags

Sie können einen vorhandenen ACE (Access Control Entry) aus einer bestimmten Datei oder einem bestimmten Ordner löschen. Die Änderung wird auf alle untergeordneten Objekte übertragen.

Schritt 1: Löschen Sie ACE

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
Löschen	/API/protocols/file-Security/permissions/{svm.uuid}/} path{

Verarbeitungsart

Asynchron

Zusätzliche Eingabeparameter für Curl-Beispiele

Neben den bei allen REST API-Aufrufen üblichen Parametern werden in diesem Schritt auch die folgenden Parameter im Curl-Beispiel verwendet.

Parameter	Typ	Erforderlich	Beschreibung
SVM_ID USD	Pfad	Ja.	Dies ist die UUID der SVM, die die Datei enthält.
PFAD FÜR DATEI	Pfad	Ja.	Dies ist der Pfad zur Datei oder zum Ordner.

Beispiel für die Wellung

```
curl --request DELETE --location "https://$FQDN_IP/api/protocols/file-
security/permissions/$SVM_ID/$FILE_PATH?return_timeout=0" --include
--header "Accept */*" --header "Authorization: Basic $BASIC_AUTH" --data
'{ \"access\": \"access_allow\", \"apply_to\": { \"files\": true,
\"sub_folders\": true, \"this_folder\": true }, \"ignore_paths\": [
\"/parent/child2\" ], \"propagation_mode\": \"propagate\"}'
```

Beispiel für eine JSON-Ausgabe

```
{
  "job": {
    "uuid": "3015c294-5bbc-11eb-9c4e-0050568e8682",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/3015c294-5bbc-11eb-9c4e-0050568e8682"
      }
    }
  }
}
```

Schritt 2: Rufen Sie den Status des Jobs ab

Führen Sie den Workflow aus "Job-Instanz abrufen" Und bestätigen Sie die `state` Wert ist `success`.

Netzwerkbetrieb

Listen Sie die IP-Schnittstellen auf

Sie können die IP-LIFs, die dem Cluster und SVMs zugewiesen sind, abrufen. Dies kann zur Bestätigung Ihrer Netzwerkkonfiguration oder beim Hinzufügen weiterer LIF notwendig sein.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
GET	/API/Netzwerk/ip/Schnittstellen

Verarbeitungsart

Synchron

Zusätzliche Eingabeparameter für die Curl-Beispiele

Zusätzlich zu den Parametern, die bei allen REST-API-Aufrufen üblich sind, werden die folgenden Parameter auch in den Curl-Beispielen für diesen Schritt verwendet.

Parameter	Typ	Erforderlich	Beschreibung
Felder	Abfrage	Nein	Geben Sie eine begrenzte Liste der relevanten Konfigurationswerte zurück.

Curl Beispiel: Gibt alle LIFs mit den Standardkonfigurationswerten zurück

```
curl --request GET \
--location "https://$FQDN_IP/api/network/ip/interfaces" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Curl Beispiel: Gibt alle LIFs mit vier spezifischen Konfigurationswerten zurück

```
curl --request GET \
--location
"https://$FQDN_IP/api/network/ip/interfaces?fields=name,scope,svm.name,ip.
address" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Beispiel für eine JSON-Ausgabe


```
{
  "records": [
    {
      "uuid": "5ded9e38-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_mgmt1",
      "ip": {
        "address": "172.29.151.116"
      },
      "scope": "cluster",
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/5ded9e38-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "bb03c162-999e-11ee-acad-005056ae6bd8",
      "name": "cluster_mgmt",
      "ip": {
        "address": "172.29.186.156"
      },
      "scope": "cluster",
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/bb03c162-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "c5ffbd03-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_data1",
      "ip": {
        "address": "172.29.186.150"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
      },
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/c5ffbd03-999e-11ee-acad-
005056ae6bd8"
```

```
        }
      }
    },
    {
      "uuid": "c6612abe-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_data2",
      "ip": {
        "address": "172.29.186.151"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
      },
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/c6612abe-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "c6b21b94-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_data3",
      "ip": {
        "address": "172.29.186.152"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
      },
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/c6b21b94-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "c7025322-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_data4",
      "ip": {
        "address": "172.29.186.153"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
```

```
      },
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/c7025322-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "c752cc66-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_data5",
      "ip": {
        "address": "172.29.186.154"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
      },
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/c752cc66-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "c7a03719-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_data6",
      "ip": {
        "address": "172.29.186.155"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
      },
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/c7a03719-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "ccd4c59c-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_data4_inet6",
      "ip": {
```

```
        "address": "fd20:8b1e:b255:300f::ac5"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
      },
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/ccd4c59c-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "d9144c30-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_data6_inet6",
      "ip": {
        "address": "fd20:8b1e:b255:300f::ac7"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
      },
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/d9144c30-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "d961c13b-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_data1_inet6",
      "ip": {
        "address": "fd20:8b1e:b255:300f::ac2"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
      },
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/d961c13b-999e-11ee-acad-
005056ae6bd8"
        }
      }
```

```
    },
    {
      "uuid": "d9ac8d6a-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_data5_inet6",
      "ip": {
        "address": "fd20:8b1e:b255:300f::ac6"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
      },
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/d9ac8d6a-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "d9fce1a3-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_data2_inet6",
      "ip": {
        "address": "fd20:8b1e:b255:300f::ac3"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
      },
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/d9fce1a3-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "da4995a0-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_data3_inet6",
      "ip": {
        "address": "fd20:8b1e:b255:300f::ac4"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
      },
      "_links": {
```

```
        "self": {
          "href": "/api/network/ip/interfaces/da4995a0-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "da9e7afd-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_cluster_mgmt_inet6",
      "ip": {
        "address": "fd20:8b1e:b255:300f::ac8"
      },
      "scope": "cluster",
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/da9e7afd-999e-11ee-acad-
005056ae6bd8"
        }
      }
    },
    {
      "uuid": "e6db58b4-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsim-sr027o_mgmt1_inet6",
      "ip": {
        "address": "fd20:8b1e:b255:3008::1a0"
      },
      "scope": "cluster",
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/e6db58b4-999e-11ee-acad-
005056ae6bd8"
        }
      }
    }
  ],
  "num_records": 16,
  "_links": {
    "self": {
      "href":
"/api/network/ip/interfaces?fields=name,scope,svm.name,ip.address"
    }
  }
}
```

Sicherheit

Konten

Auflisten der Accounts

Sie können eine Liste der Konten abrufen. Sie können dies tun, um Ihre Sicherheitsumgebung zu bewerten oder bevor Sie ein neues Konto erstellen.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
GET	/API/Sicherheit/Konten

Verarbeitungsart

Synchron

Beispiel für die Wellung

```
curl --request GET \
--location "https://$FQDN_IP/api/security/accounts" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Beispiel für eine JSON-Ausgabe


```
{
  "records": [
    {
      "owner": {
        "uuid": "642573a8-9d14-11ee-9330-005056aed3de",
        "name": "vs0",
        "_links": {
          "self": {
            "href": "/api/svm/svms/642573a8-9d14-11ee-9330-
005056aed3de"
          }
        }
      },
      "name": "vsadmin",
      "_links": {
        "self": {
          "href": "/api/security/accounts/642573a8-9d14-11ee-9330-
005056aed3de/vsadmin"
        }
      }
    },
    {
      "owner": {
        "uuid": "fdb6fe29-9d13-11ee-9330-005056aed3de",
        "name": "sti214nscluster-1"
      },
      "name": "admin",
      "_links": {
        "self": {
          "href": "/api/security/accounts/fdb6fe29-9d13-11ee-9330-
005056aed3de/admin"
        }
      }
    },
    {
      "owner": {
        "uuid": "fdb6fe29-9d13-11ee-9330-005056aed3de",
        "name": "sti214nscluster-1"
      },
      "name": "autosupport",
      "_links": {
        "self": {
          "href": "/api/security/accounts/fdb6fe29-9d13-11ee-9330-
005056aed3de/autosupport"
```

```
        }
      }
    }
  ],
  "num_records": 3,
  "_links": {
    "self": {
      "href": "/api/security/accounts"
    }
  }
}
```

Zertifikate und Schlüssel

Listen Sie die installierten Zertifikate auf

Sie können die in Ihrem ONTAP-Cluster installierten Zertifikate auflisten. Sie können damit überprüfen, ob ein bestimmtes Zertifikat verfügbar ist, oder um die ID eines bestimmten Zertifikats zu erhalten.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
GET	/API/Security/Zertifikate

Zusätzliche Eingabeparameter für Curl-Beispiele

Neben den bei allen REST API-Aufrufen üblichen Parametern werden in diesem Schritt auch die folgenden Parameter im Curl-Beispiel verwendet.

Parameter	Typ	Erforderlich	Beschreibung
max_Datensätze	Abfrage	Nein	Geben Sie die Anzahl der Datensätze an, die zurückgegeben werden sollen.

Beispiel Curl: Geben Sie drei Zertifikate zurück

```
curl --request GET \
--location "https://$FQDN_IP/api/security/certificates?max_records=3" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Beispiel für eine JSON-Ausgabe


```
{
  "records": [
    {
      "uuid": "dad822c2-573c-11ee-a310-005056aecc29",
      "name": "vs0_17866DB5C933E2EA",
      "_links": {
        "self": {
          "href": "/api/security/certificates/dad822c2-573c-11ee-a310-
005056aecc29"
        }
      }
    },
    {
      "uuid": "7d8e5570-573c-11ee-a310-005056aecc29",
      "name": "BuypassClass3RootCA",
      "_links": {
        "self": {
          "href": "/api/security/certificates/7d8e5570-573c-11ee-a310-
005056aecc29"
        }
      }
    },
    {
      "uuid": "7dbb2191-573c-11ee-a310-005056aecc29",
      "name": "EntrustRootCertificationAuthority",
      "_links": {
        "self": {
          "href": "/api/security/certificates/7dbb2191-573c-11ee-a310-
005056aecc29"
        }
      }
    }
  ],
  "num_records": 3,
  "_links": {
    "self": {
      "href": "/api/security/certificates?max_records=3"
    },
    "next": {
      "href": "/api/security/certificates?start.svm_id=sti214nscluster-
1&start.uuid=7dbb2191-573c-11ee-a310-005056aecc29&max_records=3"
    }
  }
}
```

Installieren Sie ein Zertifikat

Sie können ein signiertes X.509-Zertifikat in Ihrem ONTAP-Cluster installieren. Dies kann im Rahmen der Konfiguration einer ONTAP-Funktion oder eines Protokolls erfolgen, für das eine starke Authentifizierung erforderlich ist.

Bevor Sie beginnen

Sie müssen über das Zertifikat verfügen, das Sie installieren möchten. Stellen Sie außerdem sicher, dass alle Zwischenzertifikate bei Bedarf installiert sind.

> Bevor Sie die folgenden JSON-Eingabebeispiele verwenden, müssen Sie das aktualisieren `public_certificate` Wert mit dem Zertifikat für Ihre Umgebung.

Schritt 1: Installieren Sie das Zertifikat

Sie können einen API-Aufruf zur Installation des Zertifikats ausstellen.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
POST	/API/Security/Zertifikate

Beispiel für Curl: Installieren Sie ein Stammzertifizierungsstellenzertifikat auf Cluster-Ebene

```
curl --request POST \
--location "https://$FQDN_IP/api/security/certificates" \
--include \
--header "Content-Type: application/json" \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON-Eingabebeispiel

```
{
    "type": "server_ca",
    "public_certificate":
    "-----BEGIN CERTIFICATE-----
MIID0TCCArkCFGYdznvTVvaY1VZPNfy4yCCyPph6MA0GCSqGSIb3DQEBCwUAMIGk
MQswCQYDVQQGEwJVUzELMAkGA1UECAwCTkMxDDAKBgNVBAcMA1JUUDEWMBQGA1UE
CgwNT05UQVAgRXhhbXBsZTETMBEGA1UECwwKT05UQVAgOS4xNDEcMBoGA1UEAwwT
Ki5vbnRhcC1leGFtcGxlLmNvbTEvMC0GCSqGSIb3DQEJARYgZGF2aWQucGV0ZXJz
b25Ab250YXAtZXhhbXBsZS5jb20wHhcNMjMxMDA1MTUyOTE4WhcNMjQxMDA0MTUy
OTE4WjCBpDELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk5DMQwwCgYDVQQHDANSVFAx
FjAUBgNVBAoMDU9OVEFQIEV4YW1wbGUxEzARBgNVBAsMCk9OVEFQIDkuMTQxHDAa
BgNVBAMMEyoub250YXAtZXhhbXBsZS5jb20xLzAtBgkqhkiG9w0BCQEWIGRhdmlk
LnBldGVyc29uQG9udGFwLWV4YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAxQgy8mhb1Jhkf0D/MBodpzgW0aSp2jGbWJ+Zv2G8BXkp1762
dPHRkv1hnx9JvwkK4Dba05GiCiD5t3gjH/jUQMSFb+VwDbVmubVFnXjkm/4Q7sea
tMtA/ZpQdZbQFZ5RKtdWz7dzzPYEl2x8Q1Jc8Kh7NxERNMtgupGWZZn7mfXKYr4O
N/+vgahIhDibS8YK5rf1w6bfmrik9E2D+PEab9DX/1DL5RX4tZ1H2OkyN2UxoBR6
Fq7l6n1Hi/5yR0Oi1xStN6sO7EPoGak+KSlK41q+EcIKRo0bP4mEQp8WMjJuiTkb
5MmeYoIpWEUgJK7S0M6Tp/3bTh2CST3AWxiNxQIDAQABMA0GCSqGSIb3DQEBCwUA
A4IBAQABfBqOuROmYxdfrj93OyIiRoDcoMzvo8cHGNUsuhnlBDnL2O3qhWEs97s0
mIy6zFMGnyNYa0t4i1cFsGDKP/JuljmYHjvv+2lHWnxHjTo7AOQCnXmQH5swoDbf
o1Vjqz8Oxz+PRJ+PA3dF5/8zqaAR6QreAN/iFR++6nUq1sbbM7w03tthBVMgo/h1
E9I2jVOZsqMFujm2CYfMs4XkZtrYmN6nZA8JcUpDjIWcAVbQYurMnna9r42oS3GB
WB/FE9n+P+FfJyHJ93KGcCXbH5RF2pi3wLlHilbvVuCjLRrhJ8U20I5mZoiXvABc
IpYuBcuKXLwAarhDEacXttVjC+Bq
-----END CERTIFICATE-----"
}
```

Schritt 2: Bestätigen Sie, dass das Zertifikat installiert wurde

Führen Sie den Workflow aus "Listen Sie die installierten Zertifikate auf" Und bestätigen Sie, dass das Zertifikat verfügbar ist.

RBAC

Bereiten Sie die Verwendung von RBAC vor

Je nach Umgebung können Sie die RBAC-Funktion von ONTAP auf unterschiedliche Weise nutzen. In diesem Abschnitt werden einige gängige Szenarien als Workflows dargestellt. In jedem Fall liegt der Fokus auf einem spezifischen Sicherheits- und Verwaltungsziel.

Bevor Sie Rollen erstellen und einem ONTAP-Benutzerkonto eine Rolle zuweisen, sollten Sie die folgenden wichtigen Sicherheitsanforderungen und Optionen prüfen. Überprüfen Sie auch die allgemeinen Workflow-Konzepte unter "Die Nutzung der Workflows wird vorbereitet".

Welche ONTAP Version verwenden Sie?

Die ONTAP Version legt fest, welche REST-Endpunkte und RBAC-Funktionen verfügbar sind.

Ermittlung der geschützten Ressourcen und des Umfangs

Sie müssen die zu sichernden Ressourcen oder Befehle und den Umfang (Cluster oder SVM) festlegen.

Welchen Zugriff sollte der Benutzer haben?

Nachdem Sie die Ressourcen und den Umfang ermittelt haben, müssen Sie die zuzugeteilte Zugriffsebene festlegen.

Wie greifen die Benutzer auf ONTAP zu?

Der Benutzer kann über die REST-API oder über die CLI oder beide auf ONTAP zugreifen.

Ist eine der integrierten Rollen ausreichend oder wird eine benutzerdefinierte Rolle benötigt?

Es ist bequemer, eine vorhandene integrierte Rolle zu verwenden, aber Sie können bei Bedarf eine neue benutzerdefinierte Rolle erstellen.

Welche Art von Rolle ist erforderlich?

Basierend auf den Sicherheitsanforderungen und dem ONTAP-Zugriff müssen Sie entscheiden, ob eine REST- oder eine herkömmliche Rolle erstellt werden soll.

Erstellen Sie Rollen

Beschränkung des Zugriffs auf SVM-Volume-Vorgänge

Sie können eine Rolle definieren, um die Storage-Volume-Administration innerhalb einer SVM zu beschränken.

Informationen zu diesem Workflow

Eine herkömmliche Rolle wird zuerst erstellt, um zunächst den Zugriff auf alle wichtigen Volume-Administrationsfunktionen außer dem Klonen zu ermöglichen. Die Rolle wird mit folgenden Merkmalen definiert:

- Alle CRUD Volume-Vorgänge einschließlich get, create, modify und delete
- Volume-Klon kann nicht erstellt werden

Sie können dann optional die Rolle nach Bedarf aktualisieren. In diesem Workflow wird die Rolle im zweiten Schritt geändert, damit der Benutzer einen Volume-Klon erstellen kann.

Schritt 1: Erstellen Sie die Rolle

Sie können einen API-Aufruf ausgeben, um die RBAC-Rolle zu erstellen.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
POST	/API/Sicherheit/Funktionen

Beispiel für die Wellung

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON-Eingabebeispiel

```
{
  "name": "role1",
  "owner": {
    "name": "cluster-1",
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
      { "path": "volume create", "access": "all" },
      { "path": "volume delete", "access": "all" }
    ]
}
```

Schritt 2: Aktualisieren Sie die Rolle

Sie können einen API-Aufruf ausgeben, um die vorhandene Rolle zu aktualisieren.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
POST	/API/Sicherheit/Funktionen

Zusätzliche Eingabeparameter für Curl-Beispiele

Neben den bei allen REST API-Aufrufen üblichen Parametern werden in diesem Schritt auch die folgenden Parameter im Curl-Beispiel verwendet.

Parameter	Typ	Erforderlich	Beschreibung
SVM_ID USD	Pfad	Ja.	Dies ist die UUID der SVM, die die Rollendefinition enthält.
„ROLE_NAME“ IN US-DOLLAR	Pfad	Ja.	Dies ist der Name der Rolle innerhalb der zu aktualisierenden SVM.

Beispiel für die Wellung

```
curl --request POST \
--location
"https://$FQDN_IP/api/security/roles/$SVM_ID/$ROLE_NAME/priveleges" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON-Eingabebeispiel

```
{
  "path": "volume clone",
  "access": "all"
}
```

Administration der Datensicherung

Sie können einem Benutzer begrenzte Datensicherungsfunktionen zur Verfügung stellen.

Informationen zu diesem Workflow

Die traditionelle erstellte Rolle wird mit den folgenden Merkmalen definiert:

- Es sind möglich, Snapshots zu erstellen und zu löschen und auch SnapMirror Beziehungen zu aktualisieren
- Objekte höherer Ebene wie Volumes oder SVMs können nicht erstellt oder geändert werden

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
POST	/API/Sicherheit/Funktionen

Beispiel für die Wellung

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON-Eingabebeispiel

```
{
  "name": "role1",
  "owner": {
    "name": "cluster-1",
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
      {"path": "volume snapshot create", "access": "all"},
      {"path": "volume snapshot delete", "access": "all"},
      {"path": "volume show", "access": "readonly"},
      {"path": "vserver show", "access": "readonly"},
      {"path": "snapmirror show", "access": "readonly"},
      {"path": "snapmirror update", "access": "all"}
  ]
}
```

Erstellung von ONTAP-Berichten zulassen

Sie können EINE REST-Rolle erstellen, um Benutzern die Möglichkeit zu geben, ONTAP-Berichte zu generieren.

Informationen zu diesem Workflow

Die erstellte Rolle wird mit folgenden Merkmalen definiert:

- Abrufen aller Kapazitäts- und Performance-Objektinformationen (u. a. Volume, qtree, LUN, Aggregate, Node, Und SnapMirror Beziehungen)
- Objekte höherer Ebene (wie Volumes oder SVMs) können nicht erstellt oder geändert werden.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
POST	/API/Sicherheit/Funktionen

Beispiel für die Wellung

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON-Eingabebeispiel

```
{
  "name": "rest_role1",
  "owner": {
    "name": "cluster-1",
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
      {"path": "/api/storage/volumes", "access": "readonly"},
      {"path": "/api/storage/qtrees", "access": "readonly"},
      {"path": "/api/storage/luns", "access": "readonly"},
      {"path": "/api/storage/aggregates", "access": "readonly"},
      {"path": "/api/cluster/nodes", "access": "readonly"},
      {"path": "/api/snapmirror/relationships", "access": "readonly"},
      {"path": "/api/svm/svms", "access": "readonly"}
  ]
}
```

Erstellen Sie einen Benutzer mit einer Rolle

Sie können diesen Workflow verwenden, um einen Benutzer mit einer zugeordneten REST-Rolle zu erstellen.

Informationen zu diesem Workflow

Dieser Workflow enthält die typischen Schritte, die zum Erstellen einer benutzerdefinierten REST-Rolle und ihrer Zuordnung zu einem neuen Benutzerkonto erforderlich sind. Sowohl der Benutzer als auch die Rolle haben einen Umfang der SVM und sind einer spezifischen Daten-SVM zugeordnet. Einige der Schritte können optional sein oder müssen je nach Umgebung geändert werden.

Schritt: Listen Sie die Daten-SVMs im Cluster auf

Führen Sie den folgenden REST-API-Aufruf durch, um die SVMs im Cluster aufzulisten. Die UUID und der Name jeder SVM werden in der Ausgabe angegeben.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
GET	/API/svm/svms

Beispiel für die Wellung

```
curl --request GET \
--location "https://$FQDN_IP/api/svm/svms?order_by=name" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Nachdem Sie fertig sind

Wählen Sie die gewünschte SVM aus der Liste aus, in der Sie den neuen Benutzer und die neue Rolle erstellen möchten.

Schritt 2: Auflisten der Benutzer, die für die SVM definiert wurden

Führen Sie den folgenden REST-API-Aufruf durch, um die in der ausgewählten SVM definierten Benutzer aufzulisten. Sie können die SVM über den Eigner-Parameter angeben.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
GET	/API/Sicherheit/Konten

Beispiel für die Wellung

```
curl --request GET \
--location "https://$FQDN_IP/api/security/accounts?owner.name=dmp" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Nachdem Sie fertig sind

Wählen Sie basierend auf den bereits in der SVM definierten Benutzern einen eindeutigen Namen für den neuen Benutzer aus.

Schritt 3: Listen Sie die REST-Rollen auf, die für die SVM definiert sind

Führen Sie den folgenden REST-API-Aufruf durch, um die in der ausgewählten SVM definierten Rollen aufzulisten. Sie können die SVM über den Eigner-Parameter angeben.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
GET	/API/Sicherheit/Funktionen

Beispiel für die Wellung

```
curl --request GET \
--location "https://$FQDN_IP/api/security/roles?owner.name=dmp" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

Nachdem Sie fertig sind

Wählen Sie basierend auf den in der SVM bereits definierten Rollen einen eindeutigen Namen für die neue Rolle aus.

Schritt 4: Erstellen Sie eine benutzerdefinierte REST-Rolle

Führen Sie den folgenden REST-API-Aufruf zur Erstellung einer benutzerdefinierten REST-Rolle in der SVM aus. Die Rolle hat zunächst nur eine Berechtigung, die einen Standardzugriff von **none** schafft, so dass der Zugriff verweigert wird.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
POST	/API/Sicherheit/Funktionen

Beispiel für die Wellung

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON-Eingabebeispiel

```
{
  "name": "dprole1",
  "owner": {
    "name": "dmp",
    "uuid": "752d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
      {"path": "/api", "access": "none"},
  ]
}
```

Nachdem Sie fertig sind

Führen Sie optional Schritt 3 erneut aus, um die neue Rolle anzuzeigen. Sie können die Rollen auch in der ONTAP-CLI anzeigen.

Schritt 5: Aktualisieren Sie die Rolle, indem Sie weitere Berechtigungen hinzufügen

Führen Sie den folgenden REST-API-Aufruf durch, um die Rolle zu ändern, indem Sie nach Bedarf Berechtigungen hinzufügen.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
POST	/API/Sicherheit/Rollen/{owner.UUID}/{Name}/Privileges

Zusätzliche Eingabeparameter für Curl-Beispiele

Neben den bei allen REST API-Aufrufen üblichen Parametern werden in diesem Schritt auch die folgenden Parameter im Curl-Beispiel verwendet.

Parameter	Typ	Erforderlich	Beschreibung
SVM_ID USD	Pfad	Ja.	Die UUID der SVM, die die Rollendefinition enthält.
„ROLE_NAME“ IN US-DOLLAR	Pfad	Ja.	Der Name der Rolle in der zu aktualisierenden SVM

Beispiel für die Wellung

```
curl --request POST \
--location
"https://$FQDN_IP/api/security/roles/$SVM_ID/$ROLE_NAME/privileges" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON-Eingabebeispiel

```
{
  "path": "/api/storage/volumes",
  "access": "readonly"
}
```

Nachdem Sie fertig sind

Führen Sie optional Schritt 3 erneut aus, um die neue Rolle anzuzeigen. Sie können die Rollen auch in der ONTAP-CLI anzeigen.

Schritt 6: Erstellen Sie einen Benutzer

Führen Sie den folgenden REST-API-Aufruf zu einem Benutzerkonto erstellen aus. Die oben erstellte Rolle **dprole1** ist mit dem neuen Benutzer verknüpft.

Sie können den Benutzer ohne Rolle erstellen. In diesem Fall wird dem Benutzer eine Standardrolle zugewiesen (entweder `admin` Oder `vsadmin`) Je nachdem, ob der Benutzer mit Cluster oder SVM-Umfang definiert ist. Sie müssen den Benutzer ändern, um eine andere Rolle zuzuweisen.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
POST	/API/Sicherheit/Konten

Beispiel für die Wellung

```
curl --request POST \
--location "https://$FQDN_IP/api/security/accounts" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON-Eingabebeispiel

```
{
  "owner": {"uuid":"daf84055-248f-11ed-a23d-005056ac4fe6"},
  "name": "david",
  "applications": [
      {"application":"ssh",
       "authentication_methods":["password"],
       "second_authentication_method":"none"}
  ],
  "role":"dprole1",
  "password":"netapp123"
}
```

Nachdem Sie fertig sind

Sie können sich mit den Anmeldedaten für den neuen Benutzer bei der SVM-Managementoberfläche anmelden.

Storage

Listen Sie die Aggregate auf

Sie können eine Liste der Aggregate im Cluster abrufen. Dies könnte Sie tun, um die Auslastung und die Performance zu beurteilen.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
GET	/API/Storage/Festplatten

Verarbeitungsart

Synchron

Zusätzliche Eingabeparameter für die Curl-Beispiele

Zusätzlich zu den Parametern, die bei allen REST-API-Aufrufen üblich sind, werden die folgenden Parameter auch in den Curl-Beispielen für diesen Schritt verwendet.

Parameter	Typ	Erforderlich	Beschreibung
node.name	Abfrage	Nein	Kann verwendet werden, um den Node zu identifizieren, an den jedes Aggregat angeschlossen ist.

Beispiel Curl: Gibt alle Aggregate mit den Standardkonfigurationswerten zurück

```
curl --request GET \
--location "https://$FQDN_IP/api/storage/aggregates" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Curl Beispiel: Gibt alle Aggregate mit einem bestimmten Konfigurationswert zurück

```
curl --request GET \
--location "https://$FQDN_IP/api/storage/aggregates?fields=node.name" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Beispiel für eine JSON-Ausgabe


```
{
  "records": [
    {
      "uuid": "760d8137-fc59-47da-906a-cc28db0a1c1b",
      "name": "sti214_vsim_sr027o_aggr1",
      "node": {
        "name": "sti214-vsim-sr027o"
      },
      "_links": {
        "self": {
          "href": "/api/storage/aggregates/760d8137-fc59-47da-906a-
cc28db0a1c1b"
        }
      }
    }
  ],
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/storage/aggregates?fields=node.name"
    }
  }
}
```


Listen Sie die Festplatten auf

Sie können eine Liste der Festplatten im Cluster abrufen. Sie könnten dies tun, um eine oder mehrere Ersatzteile zu finden, die als Teil der Erstellung eines Aggregats verwendet werden.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
GET	/API/Storage/Festplatten

Verarbeitungsart

Synchron

Zusätzliche Eingabeparameter für die Curl-Beispiele

Zusätzlich zu den Parametern, die bei allen REST-API-Aufrufen üblich sind, werden die folgenden Parameter auch in den Curl-Beispielen für diesen Schritt verwendet.

Parameter	Typ	Erforderlich	Beschreibung
Bundesland	Abfrage	Nein	Kann verwendet werden, um die für neue Aggregate verfügbaren Ersatzfestplatten zu ermitteln.

Beispiel für Curl: Geben Sie alle Festplatten zurück

```
curl --request GET \
--location "https://$FQDN_IP/api/storage/disks" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Beispiel für Curl: Ersatzfestplatten zurückgeben

```
curl --request GET \
--location "https://$FQDN_IP/api/storage/disks?state=spare" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Beispiel für eine JSON-Ausgabe


```
{
  "records": [
    {
      "name": "NET-1.20",
      "state": "spare",
      "_links": {
        "self": {
          "href": "/api/storage/disks/NET-1.20"
        }
      }
    },
    {
      "name": "NET-1.12",
      "state": "spare",
      "_links": {
        "self": {
          "href": "/api/storage/disks/NET-1.12"
        }
      }
    },
    {
      "name": "NET-1.7",
      "state": "spare",
      "_links": {
        "self": {
          "href": "/api/storage/disks/NET-1.7"
        }
      }
    }
  ],
  "num_records": 3,
  "_links": {
    "self": {
      "href": "/api/storage/disks?state=spare"
    }
  }
}
```


Unterstützung

EMS

Vorbereitung auf die Verwaltung der EMS-Support-Services

Sie können die EMS-Verarbeitung (Event Management System) für einen ONTAP-Cluster konfigurieren und bei Bedarf EMS-Nachrichten abrufen.

Überblick

Es stehen verschiedene Beispiele für Workflows zur Verfügung, die die Nutzung der ONTAP EMS-Dienste veranschaulichen. Bevor Sie die Workflows verwenden und einen der REST-API-Aufrufe ausgeben, müssen Sie diese überprüfen "Die Nutzung der Workflows wird vorbereitet".

Wenn Sie Python verwenden, sehen Sie auch den Scripy "events.py" Beispiele für die Automatisierung einiger EMS-bezogener Aktivitäten.

ONTAP REST API im Vergleich zu ONTAP-CLI-Befehlen

Bei vielen Aufgaben erfordert die Verwendung der ONTAP REST-API weniger Aufrufe als die entsprechenden ONTAP CLI-Befehle. Die folgende Tabelle enthält eine Liste der API-Aufrufe und die entsprechenden CLI-Befehle, die für jede Aufgabe erforderlich sind.

ONTAP REST API	CLI VON ONTAP
/Support/ems ABRUFEN	`event config show`
POST /Support/ems/Destinations	1. `event notification destination create` 2. `event notification create`
`GET /support/ems/events`	`event log show`
`POST /support/ems/filters`	1. `event filter create -filter-name <filtername>` 2. `event filter rule add -filter-name <filtername>`

Verwandte Informationen

- "Python-Skript zur Darstellung von EMS"
- "ONTAP REST-APIs: Automatische Benachrichtigung über Ereignisse hoher Schweregrad"

Listet die EMS-Protokollereignisse auf

Sie können alle Ereignisbenachrichtigungen oder nur Meldungen mit bestimmten Merkmalen abrufen.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
GET	/API/Support/ems/Events

Verarbeitungsart

Synchron

Zusätzliche Eingabeparameter für die Curl-Beispiele

Zusätzlich zu den Parametern, die bei allen REST-API-Aufrufen üblich sind, werden die folgenden Parameter auch in den Curl-Beispielen für diesen Schritt verwendet.

Parameter	Typ	Erforderlich	Beschreibung
Felder	Abfrage	Nein	Wird verwendet, um bestimmte Felder anzufordern, die in die Antwort aufgenommen werden sollen.
max_Datensätze	Abfrage	Nein	Kann verwendet werden, um die Anzahl der in einer einzelnen Anfrage zurückgegebenen Datensätze zu begrenzen.
Log_Message	Abfrage	Nein	Wird verwendet, um nach einem bestimmten Textwert zu suchen und nur die übereinstimmenden Nachrichten zurückzugeben.
message.severity	Abfrage	Nein	Begrenzen Sie die zurückgegebenen Nachrichten auf solche mit einem bestimmten Schweregrad wie `alert`.

Beispiel Curl: Gibt die letzte Nachricht und den Namenswert zurück

```
curl --request GET \
--location
"https://$FQDN_IP/api/support/ems/events?fields=message.name&max_records=1
" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Beispiel für Curl: Gibt eine Nachricht zurück, die bestimmten Text und Schweregrad enthält

```
curl --request GET \
--location
"https://$FQDN_IP/api/support/ems/events?log_message=*disk*&message.severi
ty=alert" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Beispiel für eine JSON-Ausgabe


```
{
  "records": [
    {
      "node": {
        "name": "malha-vsim1",
        "uuid": "da4f9e62-9de3-11ec-976a-005056b369de",
        "_links": {
          "self": {
            "href": "/api/cluster/nodes/da4f9e62-9de3-11ec-976a-
005056b369de"
          }
        }
      },
      "index": 4602,
      "time": "2022-03-18T06:37:46-04:00",
      "message": {
        "severity": "alert",
        "name": "raid.autoPart.disabled"
      },
      "log_message": "raid.autoPart.disabled: Disk auto-partitioning is
disabled on this system: the system needs a minimum of 4 usable internal
hard disks.",
      "_links": {
        "self": {
          "href": "/api/support/ems/events/malha-vsim1/4602"
        }
      }
    }
  ],
  "num_records": 1,
  "_links": {
    "self": {
      "href":
"/api/support/ems/events?log_message=*disk*&message.severity=alert&max_rec
ords=1"
    },
    "next": {
      "href": "/api/support/ems/events?start.keytime=2022-03-
18T06%3A37%3A46-04%3A00&start.node.name=malha-
vsim1&start.index=4602&log_message=*disk*&message.severity=alert"
    }
  }
}
```

Rufen Sie die EMS-Konfiguration ab

Sie können die aktuelle EMS-Konfiguration für einen ONTAP-Cluster abrufen. Sie können dies tun, bevor Sie die Konfiguration aktualisieren oder eine neue EMS-Benachrichtigung erstellen.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
GET	/API/Support/ems

Verarbeitungsart

Synchron

Beispiel für die Wellung

```
curl --request GET \
--location "https://$FQDN_IP/api/support/ems" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Beispiel für eine JSON-Ausgabe

```
{
  "proxy_url": "https://proxyserver.mycompany.com",
  "proxy_user": "proxy_user",
  "mail_server": "mail@mycompany.com",
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "pubsub_enabled": "1",
  "mail_from": "administrator@mycompany.com"
}
```

Erstellen Sie eine EMS-Benachrichtigung

Sie können den folgenden Workflow verwenden, um ein neues EMS-Benachrichtigungsziel für den Empfang ausgewählter Ereignismeldungen zu erstellen.

Schritt 1: Konfigurieren Sie die systemweiten E-Mail-Einstellungen

Sie können den folgenden API-Aufruf durchführen, um die systemweiten E-Mail-Einstellungen zu konfigurieren.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
PATCH	/API/Support/ems

Verarbeitungsart

Synchron

Zusätzliche Eingabeparameter für die Curl-Beispiele

Zusätzlich zu den Parametern, die bei allen REST-API-Aufrufen üblich sind, werden die folgenden Parameter auch in den Curl-Beispielen für diesen Schritt verwendet.

Parameter	Typ	Erforderlich	Beschreibung
Mail_von	Abfrage	Ja.	Legt den fest `from` In den Benachrichtigungs-E-Mail-Nachrichten.
Mail_Server	Abfrage	Ja.	Konfiguriert den Ziel-SMTP-Mailserver.

Beispiel für die Wellung

```
curl --request PATCH \
--location
"https://$FQDN_IP/api/support/ems?mail_from=administrator@mycompany.com&mail_server=mail@mycompany.com" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Schritt 2: Definieren Sie einen Nachrichtenfilter

Sie können einen API-Aufruf ausgeben, um eine Filterregel zu definieren, die den Nachrichten entspricht.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
POST	/API/Support/ems/Filter

Verarbeitungsart

Synchron

Zusätzliche Eingabeparameter für die Curl-Beispiele

Zusätzlich zu den Parametern, die bei allen REST-API-Aufrufen üblich sind, werden die folgenden Parameter auch in den Curl-Beispielen für diesen Schritt verwendet.

Parameter	Typ	Erforderlich	Beschreibung
Filtern	Text	Ja.	Enthält die Werte für die Filterkonfiguration.

Beispiel für die Wellung

```
curl --request POST \
--location "https://$FQDN_IP/api/support/ems/filters" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON-Eingabebeispiel

```
{
  "name": "test-filter",
  "rules.type": ["include"],
  "rules.message_criteria.severities": ["emergency"]
}
```

Schritt 3: Erstellen Sie ein Nachrichtenziel

Sie können einen API-Aufruf ausgeben, um ein Nachrichtenziel zu erstellen.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
POST	/API/Support/ems/Destinations

Verarbeitungsart

Synchron

Zusätzliche Eingabeparameter für die Curl-Beispiele

Zusätzlich zu den Parametern, die bei allen REST-API-Aufrufen üblich sind, werden die folgenden Parameter auch in den Curl-Beispielen für diesen Schritt verwendet.

Parameter	Typ	Erforderlich	Beschreibung
Zielkonfiguration	Text	Ja.	Enthält die Werte für das Ereignisziel.

Beispiel für die Wellung

```
curl --request POST \
--location "https://$FQDN_IP/api/support/ems/destinations" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON-Eingabebeispiel

```
{
  "name": "test-destination",
  "type": "email",
  "destination": "administrator@mycompany.com",
  "filters.name": ["important-events"]
}
```

SVM

Listen Sie die SVMs auf

Sie können die in einem ONTAP Cluster definierten Storage Virtual Machines (SVMs) auflisten. Dies könnte dazu führen, dass Sie die Kennung für eine bestimmte SVM finden oder die Einmaligkeit des Namens sicherstellen, bevor Sie eine neue SVM erstellen.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
GET	/API/svm/svms

Beispiel für die Wellung

```
curl --request GET \
--location "https://$FQDN_IP/api/svm/svms" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Beispiel für eine JSON-Ausgabe


```
{
  "records": [
    {
      "uuid": "71bd74f8-40dc-11ee-b51a-005056aee9fa",
      "name": "vs0",
      "_links": {
          "self": {
            "href": "/api/svm/svms/71bd74f8-40dc-11ee-b51a-005056aee9fa"
          }
      }
    }
  ],
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/svm/svms"
    }
  }
}
```

Software-Tools

Python-Client-Bibliothek

Überblick über die Python Client Library

Die NetApp ONTAP Python Client Library ist ein Paket, mit dem Sie Skripts installieren und zum Schreiben von Skripten verwenden können, die auf die ONTAP REST API zugreifen. Es unterstützt mehrere zugrunde liegende Services, darunter Verbindungs-Management, asynchrone Verarbeitung, Ausnahmebehandlung und Fehlermeldungen. Mithilfe der Python-Client-Bibliothek können Sie schnell robusten Code zur Unterstützung der Automatisierung von ONTAP-Implementierungen entwickeln.

NetApp unterhält ein GitHub Repository, in dem Codebeispiele und andere hilfreiche Informationen enthalten sind. Sie können zum Ordner *examples* navigieren, um mithilfe der Python-Client-Bibliothek auf Samples zuzugreifen.

Verwandte Informationen

- "ONTAP REST Python GitHub-Repository"
- "Beispiele für die ONTAP REST Python Client-Bibliothek"

Vorbereiten der Verwendung der Python-Client-Bibliothek

Sie sollten die lokale Laufzeitumgebung vorbereiten, bevor Sie die Python-Client-Bibliothek verwenden.

Paketname und -Version

Der Name des Python Client Library-Pakets ist **netapp-ontap**. Die dem Paket zugeordnete Version ist eine Kombination aus den ONTAP-Major- und Minor-Versionsnummern, aus denen die Bibliothek erstellt wurde, sowie einer Minor-Version für den Client innerhalb der ONTAP-Version. Gültige Versionsnummern sind beispielsweise 9.6.1, 9.6 und 9.7.1.

Installation

Sie müssen pip verwenden, um das netapp_ontap Paket von der Python Package Index (PyPi) Website zu installieren.

Pakete und Dokumentation nach ONTAP Release

Jede ONTAP-Version, die mit 9.6 beginnt, verfügt über ein PyPI-Paket und die zugehörige Dokumentation. Siehe "Pakete und Dokumentation" Finden Sie weitere Informationen. Die Installationsanforderungen sind in jedem Paket enthalten und umfassen verschiedene Versionen der folgenden Komponenten:

- python
- Anträge
- Anforderungen-Werkzeuggürtel
- marshmallow

Pakete und Dokumentation

Die Python-Client-Bibliothek ist ab 9.6 für jede ONTAP-Version verfügbar. Sie sollten auf das PyPI-Paket und die Dokumentation basierend auf der von Ihnen verwendeten ONTAP-Version zugreifen.

ONTAP 9.15.1

- "PyPI: NetApp ONTAP 9.15.1"
- "NetApp PCL-Dokumentation für 9.15.1"

ONTAP 9.14.1

- "PyPI: NetApp ONTAP 9.14.1"
- "NetApp PCL-Dokumentation für 9.14.1"

ONTAP 9.13.1

- "PyPI: NetApp ONTAP 9.13.1"
- "NetApp PCL-Dokumentation für 9.13.1"

ONTAP 9.12.1

- "PyPI: NetApp ONTAP 9.12.1"
- "NetApp PCL-Dokumentation für 9.12.1"

ONTAP 9.11.1

- "PyPI: NetApp ONTAP 9.11.1"
- "NetApp PCL-Dokumentation für 9.11.1"

ONTAP 9.10.1

- "PyPI: NetApp ONTAP 9.10.1"
- "NetApp PCL-Dokumentation für 9.10.1"

ONTAP 9.9.1

- "PyPI: NetApp ONTAP 9.9.1"
- "NetApp PCL-Dokumentation für 9.9.1"

ONTAP 9.8

- "PyPI: NetApp ONTAP 9.8"
- "NetApp PCL-Dokumentation für 9.8"

ONTAP 9.7

- "PyPI: NetApp ONTAP 9.7"
- "NetApp PCL-Dokumentation für 9.7"

ONTAP 9.6

- "PyPI: NetApp ONTAP 9.6"
- "NetApp PCL-Dokumentation für 9.6"

Skript zum Abrufen der Cluster-Konfiguration

Das folgende Skript enthält ein einfaches Beispiel für die Verwendung der Python-Client-Bibliothek. Sie können das Skript mit Python 3 in der CLI ausführen, um die ONTAP-Clusterkonfiguration abzurufen.

```
##-------------------------------------------------------------------
#
# Description: Python script to retrieve the cluster configuration.
#
# Usage example:
#
# python3 get_cluster.py
#
#
# (C) Copyright 2024 NetApp, Inc.
#
# This sample code is provided AS IS, with no support or warranties of
# any kind, including but not limited for warranties of merchantability
# or fitness of any kind, expressed or implied. Permission to use,
# reproduce, modify and create derivatives of the sample code is granted
# solely for the purpose of researching, designing, developing and
# testing a software application product for use with NetApp products,
# provided that the above copyright notice appears in all copies and
# that the software application product is distributed pursuant to terms
# no less restrictive than those set forth herein.
#
##-------------------------------------------------------------------
# For reading the password from the commandline
from getpass import getpass
# Global configuration for the library
from netapp_ontap import config
# Support for the connection to ONTAP
from netapp_ontap import HostConnection
# Specific API needed for this script
from netapp_ontap.resources import Cluster
# Create connection to the ONTAP management LIF
# (add verify=False if the certificate your cluster is serving is not
trusted)
conn = HostConnection(
    "<mgmt_ip>", username="admin", password=getpass("ONTAP admin password:
"),
)
# Set connection as the default for all API calls
config.CONNECTION = conn
# Create new cluster object
clus = Cluster()
# Issue REST API call
clus.get()
# Display the cluster configuration
print(clus)
```

Blog-Artikel

Es gibt mehrere Blog-Artikel, die Ihnen helfen, besser zu verstehen, wie man die Python Client-Bibliothek verwendet.

Vereinfachte ONTAP-REST-API-Nutzung mit der Python Client-Bibliothek

Dieser Blog bietet eine gute Einführung in die Funktionen der ONTAP Python Client Library.

"www.netapp.com/blog/simplify-ontap-rest-api-consumption"

Erste Schritte mit der ONTAP REST API Python Client Library

Dies ist eine dreiteilige Reihe von Blogs, die mehr Details über die Python Client-Bibliothek behandeln.

Teil 1: "netapp.io/2020/06/09/ontap-Rest-API-Python-Client-Library-pt1"

Teil 2: "netapp.io/2020/06/09/ontap-Rest-API-Python-Client-Library-pt2/"

Teil 3: "netapp.io/2020/06/09/ontap-Rest-API-Python-Client-Library-pt3"

PowerShell Toolkit

Überblick über das PowerShell Toolkit

NetApp unterstützt die Verwendung von PowerShell für das Management von ONTAP Storage-Systemen.

PowerShell

PowerShell ist ein Programm von Microsoft, das Sie zur Aufgabenautomatisierung und zum Konfigurationsmanagement verwenden können. Es umfasst eine Kommandozeilen-Shell-Umgebung sowie eine Skriptsprache.

NetApp ONTAP PowerShell Toolkit

Das NetApp. Das ONTAP PowerShell Toolkit enthält das PowerShell Modul für NetApp ONTAP. Das Toolkit unterstützt ONTAP in einer Vielzahl von Umgebungen, darunter NetApp AFF und FAS Systeme, Standard-Hardware und die Cloud. Das Modul enthält über 2,400 Cmdlets, die gemeinsam die Speicheradministration auf Windows-Hosts unterstützen.

Laden Sie das PowerShell Toolkit herunter, und installieren Sie es

Es gibt zwei Optionen zum Herunterladen und Installieren des NetApp ONTAP PowerShell Toolkits.

NetApp Support

Sie können das PowerShell Toolkit von der NetApp Support-Website herunterladen:

https://mysupport.netapp.com/site/tools/tool-eula/ontap-powershell-toolkit

PowerShell Galerie

Sie können das PowerShell Toolkit von der PowerShell Galerie herunterladen:

https://www.powershellgallery.com/packages/NetApp.ONTAP/9.12.1.2302

NetApp Manageability SDK

Das NetApp Manageability SDK bietet eine Reihe von ONTAPI-Aufrufen für die Entwicklung von Applikationen, um Ihren ONTAP Storage zu überwachen und zu managen. Zusammen mit dem OnCommand Workflow Automation-Paket unterstützt das SDK Ihre Bemühungen, das Management Ihrer ONTAP Systeme zu automatisieren.

Während das NetApp Manageability SDK und die OnCommand Workflow Automation weiterhin unterstützt werden, ist die ONTAP REST API die bevorzugte und strategische Technologie für die Automatisierung Ihrer ONTAP Systeme. Siehe "ONTAPI Deaktivierung" Finden Sie weitere Informationen.

SDK herunterladen

Sie können das NetApp Manageability SDK von der NetApp Support-Website herunterladen. Das SDK unterstützt mehrere Sprachen auf der Client-Seite, darunter: Python, PowerShell, C, C++, Java, C#, VB. NET und Ruby. Im Interoperabilitäts-Matrix-Tool finden Sie Informationen zum NetApp Manageability SDK und zur Unterstützung durch Ihre Version von ONTAP.

Verwenden Sie OnCommand Workflow Automation

Sie können die mit dem SDK bereitgestellte API auch verwenden, um Managementaufgaben zu automatisieren, ohne Skripts schreiben zu müssen. OnCommand Workflow Automation (OnCommand WFA) bietet mehrere vorgefertigte Workflows für die Implementierung und Ausführung von Managementaufgaben. Sie können das OnCommand WFA Paket aus dem NetApp Storage Automation Store herunterladen.

Verwandte Informationen

- "NetApp Support Website"
- "NetApp Interoperabilitäts-Matrix-Tool"
- "NetApp Manageability SDK-Dokumentation"
- "OnCommand Workflow Automation Dokumentationsressourcen"
- "NetApp Automation Store"

Migrieren Sie von ONTAPI zur REST-API

ONTAPI Deaktivierung

Die ONTAPI API (ZAPI) ist die ursprüngliche Gruppe proprietärer Aufrufe, die in der NetApp ONTAP Software enthalten sind. Die API wird über das Network Manageability SDK bereitgestellt und unterstützt die Automatisierung von Storage-Administrations- und Managementaufgaben. Die ONTAPI Schnittstelle wird in zukünftigen Versionen von ONTAP deaktiviert. Wenn Sie ONTAPI verwenden, sollten Sie die Migration zur ONTAP REST-API planen.

Verwandte Informationen

- "ONTAP-Automatisierungsoptionen"
- "Einstellung des Angebots für CPC-00410: ONTAPI"
- "FAQs zur ZAPI-zu-ONTAP-REST-API-Transformation für CPC"

Überlegungen zur Migration

Vor der Migration zur ONTAP-REST-API von entweder der ONTAPI (ZAPI) oder der ONTAP-CLI sollten Sie mehrere Probleme in Betracht ziehen.

Allgemeine Designunterschiede

Die ONTAP REST API und die Befehlszeilenschnittstelle haben ein grundlegend anderes Design. Die CLI-Befehle und -Parameter werden den REST-API-Aufrufen nicht direkt zugeordnet. Und auch wenn es eine Ähnlichkeit geben könnte, können die Details der Eingabeparameter unterschiedlich sein. Beispielsweise können numerische Einheiten in Byte oder mit einem Suffix (z. B. KB) angegeben werden. Siehe "Eingabevariablen, die eine API-Anforderung steuern" Und "API-Referenz" Finden Sie weitere Informationen.

Data-SVMs werden über DIE REST-API offengelegt

ONTAP unterstützt mehrere Arten von Storage Virtual Machines (SVMs). Allerdings sind nur die Daten-SVMs direkt über die ONTAP REST API zugänglich. Die Konfigurationsinformationen, die das Cluster und die Nodes beschreiben, sind über die REST-API verfügbar. Das Cluster und die Nodes werden jedoch nicht als separate SVMs behandelt.

Greifen Sie über die REST API auf die ONTAP-CLI zu

ONTAP bietet einen REST-Endpunkt für den Zugriff auf die ONTAP-CLI, um die ONTAPI und CLI-Benutzer bei der Transition zur ONTAP-REST-API zu unterstützen. Sie können diese Passthrough-Funktion verwenden, um jeden CLI-Befehl auszuführen. Die Nutzung des REST-Endpunkts wird in den AutoSupport-Daten zurückgegeben, damit NetApp Lücken in der REST-API identifizieren und in künftigen ONTAP-Versionen Verbesserungen vornehmen kann.

Um einen CLI-Befehl auszustellen, müssen Sie einen REST API-Aufruf machen, der ordnungsgemäß basierend auf Regeln bezüglich folgender Punkte gebildet wird:

- Ressourcenpfade

- Feldnamen
- HTTP-Methoden

Der grundlegende Ressourcenpfad für CLI-Zugriff ist `/private/cli`. Informationen zum Zugriff auf die CLI über DIE REST-API finden Sie auf der ONTAP-API-Seite mit der Online-Dokumentation. NetApp unterhält zudem ein GitHub-Repository mit Codebeispielen und anderen nützlichen Informationen. Siehe "ONTAP REST Python GitHub-Repository - CLI-Passthrough-Samples" Finden Sie weitere Informationen.

Änderungen an der SnapDiff Availability in ONTAPI

Ab ONTAP 9.10.1 können die ONTAPI Aufrufe von SnapDiff v1 und v2 nicht aufgerufen werden. Alle Anwendungen von Drittanbietern, die SnapDiff v1 oder v2 ONTAPI Aufrufe aufrufen, funktionieren nicht ab ONTAP 9.10.1. ONTAP Benutzer sollten vor einem Upgrade auf ONTAP 9.10.1 überprüfen, ob ihre Backup-Applikation die SNAPDIFF v3-REST-Aufrufe unterstützt.

Die SnapDiff API-Verfügbarkeit aller ONTAP-Versionen ist wie folgt definiert:

- ONTAP 9.7 und frühere Versionen: v1 und v2 (nur ONTAPI)
- ONTAP 9.8 – 9.9.1: v1, v2 und v3 (sowohl ONTAPI als auch REST API)
- ONTAP 9.10.1: Nur v3 (NUR REST API)

Siehe auch "Versionshinweise zu ONTAP" Finden Sie weitere Informationen.

Übermitteln Sie Ihre ONTAPI-Lücken in der REST-API

NetApp unterstützt unsere Kunden engagiert bei der Migration von ONTAP zur ONTAP REST-API. Wenn Sie etwas in der REST-API fehlt bemerken, lassen Sie es uns bitte wissen. Sie können diese Lücken und andere Ideen auf der einreichen "ONTAPI FÜR REST-API" Seite.

ONTAPI-to-REST-API-Zuordnung

Die ONTAP REST API umfasst Funktionen, die in den meisten Bereichen ONTAPI entsprechen. NetApp bietet Dokumentation, die die Zuordnung von ONTAPI-Aufrufen zu äquivalenten REST-API-Aufrufen beschreibt.

Die Dokumentation für die API-Zuordnung ist abhängig von der ONTAP Version:

- "ONTAP 9.15.1"
- "ONTAP 9.14.1"
- "ONTAP 9.13.1"
- "ONTAP 9.12.1"
- "ONTAP 9.11.1"
- "ONTAP 9.10.1"
- "ONTAP 9.9.1"
- "ONTAP 9.8"

Performance-Zähler

Der ONTAP Zählermanager enthält umfassende Informationen zur Performance jedes ONTAP Systems. Diese Daten werden als Reihe von *Performance-Zählern* exportiert, mit denen Sie die Performance Ihres ONTAP Systems einschätzen und Ihre Performance-Ziele erreichen können.

Greifen Sie auf die ONTAP-Leistungszähler zu

Sie können über zwei verschiedene APIs sowie über die ONTAP-Befehlszeilenschnittstelle auf die ONTAP-Leistungszähler zugreifen.

Die ONTAP REST-API ist die bevorzugte und strategische Option für die Automatisierung der Administration Ihrer ONTAP Implementierungen.

ONTAPI API

Die ONTAPI ist mit dem NetApp Network Manageability SDK verfügbar. Bei Verwendung von ONTAPI werden die Leistungsindikatoren in einer Sammlung von Objekten definiert. Jedes Objekt entspricht einer physischen oder virtuellen Komponente des Systems. Basierend auf der Systemkonfiguration kann ein oder mehrere Instanzen jedes Objekts vorhanden sein.

Wenn Ihr ONTAP-System beispielsweise vier physische Festplatten hat, gibt es vier Instanzen von `disk` Objekt mit jeweils einem eigenen Satz an Performance-Zählern. Über ONTAPI können Sie auf die einzelnen Zähler für jede Festplatteninstanz zugreifen.

ONTAP REST API

Ab ONTAP 9.11.1 können Sie auch über DIE REST-API auf die Performance-Daten zugreifen. In diesem Fall sind die Leistungszähler in Tabellen organisiert, die den ONTAPI-Objekten entsprechen. Jede Tabellenzeile entspricht einer Instanz eines ONTAPI-Objekts.

Wenn Ihr ONTAP-System beispielsweise vier physische Festplatten hat, wird der angezeigt `disk` Die Tabelle enthält vier Zeilen. Jede Zeile kann einzeln aufgerufen werden und enthält eine eigene Reihe von Leistungsindikatoren, die als Felder oder Spalten in der Zeile verfügbar sind.

Die Verwendung der REST-API wird vorbereitet

Sie sollten sich vor der Verwendung der ONTAP REST API vorbereiten, um auf die Performance-Zähler zuzugreifen.

Leistungszähler sind in Tabellen organisiert

Eine Untergruppe der ONTAPI Objekte ist über die ONTAP REST API verfügbar und als Tabellen dargestellt. Zum Beispiel wird das ONTAPI **hostadapter**-Objekt über DIE REST-API als **Host_adpater**-Tabelle dargestellt. Jeder Host Adapter im System ist eine Reihe mit eigenen Performance-Zählern.

Instanzname	Performance-Zähler					
Host_Adapter_1	Total_read_OPS_1	Total_write_OPS_1	Bytes_read_1	Bytes_written_1	max_Link_Data_Rate_1	rscn_count_1

Instanzname	Performance-Zähler					
Host_Adapter_2	Total_read_OPS_2	Total_write_OPS_2	Bytes_read_2	Bytes_written_2	max_Link_Data_Rate_2	rscn_count_2
Host_Adapter_3	Total_read_OPS_3	Total_write_OPS_3	Byte_Read_3	Bytes_written_3	max_Link_Data_Rate_3	rscn_count_3

Zusammenfassung der REST-Endpunkte

Für den Zugriff auf die ONTAP-Leistungszähler und zugehörige Tabellen stehen vier Hauptendpunkte zur Verfügung.

Jeder REST-Endpunkt bietet schreibgeschützten Zugriff und unterstützt nur die HTTP-Methode **GET**. Siehe "API-Referenz" Finden Sie weitere Informationen.

- **/Cluster/Zähler/Tabellen**

  Gibt eine Sammlung von Zählertabellen und deren Schemadefinitionen zurück.

- **/Cluster/Zähler/Tabellen/{Name}**

  Gibt Informationen über eine einzelne angegebene Zählertabelle zurück.

- **/Cluster/counter/tables/{counter_Name}/rows**

  Gibt eine Sammlung von Zeilen aus einer benannten Zählertabelle zurück.

- **/Cluster/Zähler/Tabellen/{counter_Name}/rows/{id}**

  Gibt eine bestimmte Zeile aus einer benannten Zählertabelle zurück.

Migration von ONTAPI zu REST API

NetApp bietet umfassenden Support für die Migration Ihres Automatisierungscodes von ONTAPI auf die ONTAP REST API. Dazu gehört auch die Zuordnungsdokumentation zur Identifikation der äquivalenten Leistungstabelle, die in DER REST-API für ein bestimmtes ONTAPI-Objekt verfügbar ist.

Finden Sie in der entsprechenden Dokumentation für die Zuordnung auf der Grundlage der ONTAP Version, die Sie verwenden:

- "ONTAP 9.15.1 Performance Counter Mapping"
- "ONTAP 9.14.1 Performance Counter Mapping"
- "ONTAP 9.13.1 Performance Counter Mapping"
- "ONTAP 9.12.1 Zählerzuordnung der Performance"
- "ONTAP 9.11.1 Zählerzuordnung der Performance"

Erste Schritte mit der ONTAP REST API

Die folgenden Beispiele veranschaulichen die Verwendung DER REST-API für den Zugriff auf die ONTAP-Performance-Zähler. Dazu gehört das Abrufen einer Liste der verfügbaren Tabellen und das Erforschen der Tabellenstruktur.

Bevor Sie beginnen

Lesen Sie die folgenden Informationen durch, bevor Sie die Beispiele verwenden.

ONTAP Referenzen

Sie benötigen ein ONTAP-Administratorkonto mit dem Kennwort.

Cluster-Management-IP

Sie benötigen die für Ihr ONTAP System konfigurierte Cluster-Management-IP-Adresse.

Alle API-Aufrufe verwenden die GET-Methode

Alle unten aufgeführten Beispiele können nur verwendet werden, um Informationen mit der HTTP GET-Methode abzurufen.

Variablenersatz

Jedes Curl-Beispiel enthält eine oder mehrere Variablen, wie sie mit Kapitalien und Text in Klammern angegeben sind. Stellen Sie sicher, dass diese Variablen durch tatsächliche Werte ersetzt werden, die für Ihre Umgebung geeignet sind.

Beispiele stimmen mit den Endpunkten überein

Die nachfolgende Beispielsequenz zeigt, wie die RESTLICHEN Endpunkte zum Abrufen der Leistungszähler verwendet werden. Siehe Zusammenfassung der REST-Endpunkte Finden Sie weitere Informationen.

Beispiel 1: Alle Performance-Zählertabellen

Sie können diesen REST-API-Aufruf verwenden, um alle verfügbaren Zählermanager-Tabellen zu ermitteln.

Beispiel für die Wellung

```
curl --request GET --user admin:<PASSWORD>
'https://<ONTAP_IP_ADDRESS>/api/cluster/counter/tables'
```

Beispiel für eine JSON-Ausgabe


```
{
  "records": [
    {
      "name": "copy_manager",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/copy_manager"
        }
      }
    },
    {
      "name": "copy_manager:constituent",
      "_links": {
        "self": {
          "href":
"/api/cluster/counter/tables/copy_manager%3Aconstituent"
        }
      }
    },
    {
      "name": "disk",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/disk"
        }
      }
    },
    {
      "name": "disk:constituent",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/disk%3Aconstituent"
        }
      }
    },
    {
      "name": "disk:raid_group",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/disk%3Araid_group"
        }
      }
    },
    {
```

```
      "name": "external_cache",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/external_cache"
        }
      }
    },
    {
      "name": "fcp",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/fcp"
        }
      }
    },
    {
      "name": "fcp:node",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/fcp%3Anode"
        }
      }
    },
    {
      "name": "fcp_lif",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/fcp_lif"
        }
      }
    },
    {
      "name": "fcp_lif:node",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/fcp_lif%3Anode"
        }
      }
    },
    {
      "name": "fcp_lif:port",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/fcp_lif%3Aport"
        }
      }
```

```
    },
    {
      "name": "fcp_lif:svm",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/fcp_lif%3Asvm"
        }
      }
    },
    {
      "name": "fcvi",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/fcvi"
        }
      }
    },
    {
      "name": "headroom_aggregate",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/headroom_aggregate"
        }
      }
    },
    {
      "name": "headroom_cpu",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/headroom_cpu"
        }
      }
    },
    {
      "name": "host_adapter",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/host_adapter"
        }
      }
    },
    {
      "name": "iscsi_lif",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/iscsi_lif"
```

```
      }
    }
  },
  {
    "name": "iscsi_lif:node",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/iscsi_lif%3Anode"
      }
    }
  },
  {
    "name": "iscsi_lif:svm",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/iscsi_lif%3Asvm"
      }
    }
  },
  {
    "name": "lif",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/lif"
      }
    }
  },
  {
    "name": "lif:svm",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/lif%3Asvm"
      }
    }
  },
  {
    "name": "lun",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/lun"
      }
    }
  },
  {
    "name": "lun:constituent",
    "_links": {
```

```
        "self": {
          "href": "/api/cluster/counter/tables/lun%3Aconstituent"
        }
      }
    },
    {
      "name": "lun:node",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/lun%3Anode"
        }
      }
    },
    {
      "name": "namespace",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/namespace"
        }
      }
    },
    {
      "name": "namespace:constituent",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/namespace%3Aconstituent"
        }
      }
    },
    {
      "name": "nfs_v4_diag",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/nfs_v4_diag"
        }
      }
    },
    {
      "name": "nic_common",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/nic_common"
        }
      }
    },
    {
```

```
      "name": "nvmf_lif",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/nvmf_lif"
        }
      }
    },
    {
      "name": "nvmf_lif:constituent",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/nvmf_lif%3Aconstituent"
        }
      }
    },
    {
      "name": "nvmf_lif:node",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/nvmf_lif%3Anode"
        }
      }
    },
    {
      "name": "nvmf_lif:port",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/nvmf_lif%3Aport"
        }
      }
    },
    {
      "name": "object_store_client_op",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/object_store_client_op"
        }
      }
    },
    {
      "name": "path",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/path"
        }
      }
```

```
    },
    {
      "name": "processor",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/processor"
        }
      }
    },
    {
      "name": "processor:node",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/processor%3Anode"
        }
      }
    },
    {
      "name": "qos",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/qos"
        }
      }
    },
    {
      "name": "qos:constituent",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/qos%3Aconstituent"
        }
      }
    },
    {
      "name": "qos:policy_group",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/qos%3Apolicy_group"
        }
      }
    },
    {
      "name": "qos_detail",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/qos_detail"
```

```
        }
      }
    },
    {
      "name": "qos_detail_volume",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/qos_detail_volume"
        }
      }
    },
    {
      "name": "qos_volume",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/qos_volume"
        }
      }
    },
    {
      "name": "qos_volume:constituent",
      "_links": {
        "self": {
          "href":
"/api/cluster/counter/tables/qos_volume%3Aconstituent"
        }
      }
    },
    {
      "name": "qtree",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/qtree"
        }
      }
    },
    {
      "name": "qtree:constituent",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/qtree%3Aconstituent"
        }
      }
    },
    {
      "name": "svm_cifs",
```

```
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/svm_cifs"
        }
      }
    },
    {
      "name": "svm_cifs:constituent",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/svm_cifs%3Aconstituent"
        }
      }
    },
    {
      "name": "svm_cifs:node",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/svm_cifs%3Anode"
        }
      }
    },
    {
      "name": "svm_nfs_v3",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/svm_nfs_v3"
        }
      }
    },
    {
      "name": "svm_nfs_v3:constituent",
      "_links": {
        "self": {
          "href":
"/api/cluster/counter/tables/svm_nfs_v3%3Aconstituent"
        }
      }
    },
    {
      "name": "svm_nfs_v3:node",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/svm_nfs_v3%3Anode"
        }
      }
```

```
    },
    {
      "name": "svm_nfs_v4",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/svm_nfs_v4"
        }
      }
    },
    {
      "name": "svm_nfs_v41",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/svm_nfs_v41"
        }
      }
    },
    {
      "name": "svm_nfs_v41:constituent",
      "_links": {
        "self": {
          "href":
"/api/cluster/counter/tables/svm_nfs_v41%3Aconstituent"
        }
      }
    },
    {
      "name": "svm_nfs_v41:node",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/svm_nfs_v41%3Anode"
        }
      }
    },
    {
      "name": "svm_nfs_v42",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/svm_nfs_v42"
        }
      }
    },
    {
      "name": "svm_nfs_v42:constituent",
      "_links": {
        "self": {
```

```
          "href":
"/api/cluster/counter/tables/svm_nfs_v42%3Aconstituent"
        }
      }
    },
    {
      "name": "svm_nfs_v42:node",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/svm_nfs_v42%3Anode"
        }
      }
    },
    {
      "name": "svm_nfs_v4:constituent",
      "_links": {
        "self": {
          "href":
"/api/cluster/counter/tables/svm_nfs_v4%3Aconstituent"
        }
      }
    },
    {
      "name": "svm_nfs_v4:node",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/svm_nfs_v4%3Anode"
        }
      }
    },
    {
      "name": "system",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/system"
        }
      }
    },
    {
      "name": "system:constituent",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/system%3Aconstituent"
        }
      }
    },
```

```
    {
      "name": "system:node",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/system%3Anode"
        }
      }
    },
    {
      "name": "token_manager",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/token_manager"
        }
      }
    },
    {
      "name": "volume",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/volume"
        }
      }
    },
    {
      "name": "volume:node",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/volume%3Anode"
        }
      }
    },
    {
      "name": "volume:svm",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/volume%3Asvm"
        }
      }
    },
    {
      "name": "wafl",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/wafl"
        }
```

```
      }
    },
    {
      "name": "wafl_comp_aggr_vol_bin",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/wafl_comp_aggr_vol_bin"
        }
      }
    },
    {
      "name": "wafl_hya_per_aggregate",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/wafl_hya_per_aggregate"
        }
      }
    },
    {
      "name": "wafl_hya_sizer",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/wafl_hya_sizer"
        }
      }
    }
  ],
  "num_records": 71,
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables"
    }
  }
}
```


Beispiel 2: Allgemeine Informationen zu einer bestimmten Tabelle

Sie können diesen REST-API-Aufruf verwenden, um die Beschreibung und Metadaten für eine bestimmte Tabelle anzuzeigen. Die Ausgabe enthält den Zweck der Tabelle und welche Art von Daten jeder Performance-Zähler enthält. In diesem Beispiel wird die Tabelle **Host_Adapter** verwendet.

Beispiel für die Wellung

```
curl --request GET --user admin:<PASSWORD>
'https://<ONTAP_IP_ADDRESS>/api/cluster/counter/tables/host_adapter'
```

Beispiel für eine JSON-Ausgabe


```
{
  "name": "host_adapter",
  "description": "The host_adapter table reports activity on the Fibre
Channel, Serial Attached SCSI, and parallel SCSI host adapters the
storage system uses to connect to disks and tape drives.",
  "counter_schemas": [
    {
      "name": "bytes_read",
      "description": "Bytes read through a host adapter",
      "type": "rate",
      "unit": "per_sec"
    },
    {
      "name": "bytes_written",
      "description": "Bytes written through a host adapter",
      "type": "rate",
      "unit": "per_sec"
    },
    {
      "name": "max_link_data_rate",
      "description": "Max link data rate in Kilobytes per second for a
host adapter",
      "type": "raw",
      "unit": "kb_per_sec"
    },
    {
      "name": "node.name",
      "description": "System node name",
      "type": "string",
      "unit": "none"
    },
    {
      "name": "rscn_count",
      "description": "Number of RSCN(s) received by the FC HBA",
      "type": "raw",
      "unit": "none"
    },
    {
      "name": "total_read_ops",
      "description": "Total number of reads on a host adapter",
      "type": "rate",
      "unit": "per_sec"
    },
    {
```

```
      "name": "total_write_ops",
      "description": "Total number of writes on a host adapter",
      "type": "rate",
      "unit": "per_sec"
    }
  ],
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/host_adapter"
    }
  }
}
```


Beispiel 3: Alle Zeilen in einer bestimmten Tabelle

Mit diesem REST-API-Aufruf können Sie alle Zeilen in einer Tabelle anzeigen. Dies gibt an, welche Instanzen der Counter Manager-Objekte vorhanden sind.

Beispiel für die Wellung

```
curl --request GET --user admin:<PASSWORD>
'https://<ONTAP_IP_ADDRESS>/api/cluster/counter/tables/host_adapter/row
s'
```

Beispiel für eine JSON-Ausgabe


```
{
  "records": [
    {
      "id": "dmp-adapter-01",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/host_adapter/rows/dmp-
adapter-01"
        }
      }
    },
    {
      "id": "dmp-adapter-02",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/host_adapter/rows/dmp-
adapter-02"
        }
      }
    }
  ],
  "num_records": 2,
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/host_adapter/rows"
    }
  }
}
```


Beispiel 4: Einzelne Zeile in einer bestimmten Tabelle

Mit diesem REST-API-Aufruf können Sie Performance-Zählerwerte für eine bestimmte Zählermanager-Instanz in der Tabelle anzeigen. In diesem Beispiel werden die Performance-Daten für einen der Host-Adapter angefordert.

Beispiel für die Wellung

```
curl --request GET --user admin:<PASSWORD>
'https://<ONTAP_IP_ADDRESS>/api/cluster/counter/tables/host_adapter/row
s/dmp-adapter-01'
```

Beispiel für eine JSON-Ausgabe

```
{
  "counter_table": {
    "name": "host_adapter"
  },
  "id": "dmp-adapter-01",
  "properties": [
    {
      "name": "node.name",
      "value": "dmp-node-01"
    }
  ],
  "counters": [
    {
      "name": "total_read_ops",
      "value": 25098
    },
    {
      "name": "total_write_ops",
      "value": 48925
    },
    {
      "name": "bytes_read",
      "value": 1003799680
    },
    {
      "name": "bytes_written",
      "value": 6900961600
    },
    {
      "name": "max_link_data_rate",
      "value": 0
    },
    {
      "name": "rscn_count",
      "value": 0
    }
  ],
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/host_adapter/rows/dmp-
adapter-01"
    }
  }
}
```

Tools und Software von NetApp

NetApp bietet Beispiel-Python-Skripts und andere damit verbundene Software zur Unterstützung Ihrer Migration von ONTAP zur ONTAP REST-API. Die wichtigsten dieser Proben werden im Folgenden beschrieben.

Alle Python-Codebeispiele sind auf der verfügbar "NetApp ONTAP REST Python" GitHub Repository:

ONTAPI Tool zur Berichterstellung zur Nutzung

Das ONTAPI Tool zur Nutzungsberichterstellung soll NetApp Professional Services, Kunden und Partner bei der Identifizierung der ONTAPI-Nutzung in ihrer ONTAP Umgebung unterstützen. Skripts werden für drei verschiedene Anwendungsfälle bereitgestellt, wie in der folgenden Tabelle beschrieben.

Skript	Beschreibung
apache_scraper.py	Ein Apache-Protokollabstreifer, um die ONTAPI-Aufrufe zu finden, die für die ONTAP-Knoten ausgegeben werden
session_stats.py	Ein CLI-Skript zum Abrufen von Sitzungsstatistikdaten aus ONTAP
zapi_to_rest.py	Ein Skript, um die RESTLICHEN Details der ONTAPI-Aufrufe und übergebenen Attribute zu extrahieren

Sie können auf das zugreifen "ONTAPI Tool zur Berichterstellung zur Nutzung" Und legen Sie los. Siehe auch A "Demo" Das Reporting-Tool und seine Verwendung.

Private CLI-Passthrough

Die REST-API bietet umfassende Abdeckung der Funktionen und Einrichtungen von ONTAP. Es kann jedoch vorkommen, dass ein direkter Zugriff über die REST-API auf die ONTAP-CLI nützlich sein kann.

Eine Einführung zu dieser Funktion finden Sie unter "Greifen Sie über die REST API auf die ONTAP-CLI zu". Für die Python-Beispiele siehe "REST CLI-Passthrough-Beispiele".

Python-Client-Bibliothek

Die Python-Client-Bibliothek ist ein Paket, das Sie installieren und verwenden können, um auf die ONTAP-REST-API mit Python zuzugreifen. Mit ihr können Sie schnell und robusten Code für die Automatisierung Ihrer ONTAP Implementierungen entwickeln.

Eine Einführung in die Python Client-Bibliothek finden Sie unter "Überblick über die Python Client Library". Für die Python-Beispiele siehe "Beispiele für Python Client-Bibliotheken".

ONTAP PowerShell Toolkit

Das NetApp.ONTAP PowerShell Toolkit erweitert Ihre lokale PowerShell Umgebung um ein Modul mit mehr als 2,400 Commandlets. Damit können Sie schnell Code für Ihren Windows-Host entwickeln und die ONTAP-Bereitstellungen automatisieren. Weitere Informationen finden Sie unter "Überblick über das PowerShell Toolkit".

Blog-Artikel

Es gibt mehrere Blog-Artikel, die Ihnen dabei helfen, besser zu verstehen, wie Sie von ONTAPI auf die ONTAP REST API migrieren.

ONTAPI zu REST Mapping

NetApp bietet Unterstützung beim Wechsel von der proprietären ONTAPI API API zur ONTAP REST API durch Mapping-Dokumentation.

"netapp.io/2020/12/17/ontapi-zu-Rest-Zuordnung"

Umwandlung Ihrer Automatisierung in eine ONTAP REST-API von ONTAPI

Es stehen verschiedene Technologien zur Verfügung, mit denen Sie Ihre ONTAP-Automatisierungsumgebung auf Basis der REST-API transformieren können.

"www.netapp.com/blog/transform-automation-ontap-rest-api"

Verwenden des privaten CLI-Passthrough mit der ONTAP REST API

Damit CLI- und ONTAP-Benutzer die Transition auf die ONTAP REST API erleichtern, bietet ONTAP einen privaten REST-API-Endpunkt, über den auf jeden CLI-Befehl zugegriffen werden kann.

"https://netapp.io/2020/11/09/private-cli-passthrough-ontap-rest-api"

Wechsel von ONTAPI mithilfe des ONTAPI Usage Reporting Tools

NetApp bietet ein Tool, das Kunden und Partner beim Wechsel zur ONTAP REST API unterstützt.

"netapp.io/2022/03/21/Transition-from-ontapizapi-using-ontapi-Usage-Reporting-Tool"

API-Referenz

Die API-Referenz enthält Details zu den ONTAP-REST-API-Aufrufen, einschließlich der HTTP-Methoden, Eingabeparameter und Antworten. Diese vollständige Referenz ist hilfreich, wenn Automatisierungsapplikationen mithilfe der REST API entwickelt werden.

Die REST-API-Referenzdokumentation ist an mehreren Standorten verfügbar, die auf der ONTAP Version basieren. Eine Kopie der entsprechenden Dokumentation ist auch über die Swagger-Benutzeroberfläche auf Ihrem lokalen ONTAP-System verfügbar.

Die Referenzdokumentation zur ONTAP API ist online verfügbar

Sie können über die unten angegebenen Links auf eine Kopie der Referenzdokumentation für die ONTAP REST-API zugreifen. Die Dokumentation wird durch die ONTAP-Version gepflegt.

- "ONTAP 9.15.1"
- "ONTAP 9.14.1"
- "ONTAP 9.13.1"
- "ONTAP 9.12.1"
- "ONTAP 9.11.1"
- "ONTAP 9.10.1"
- "ONTAP 9.9.1"
- "ONTAP 9.8"
- "ONTAP 9.7"
- "ONTAP 9.6"

Greifen Sie über die Swagger-Benutzeroberfläche auf die Referenzdokumentation zur ONTAP-API zu

Sie können über die Swagger-Benutzeroberfläche Ihres lokalen ONTAP-Systems auf die ONTAP-REST-API-Dokumentation zugreifen.

Bevor Sie beginnen

Sie müssen Folgendes haben:

- IP-Adresse oder Host-Name der ONTAP Cluster-Management-LIF
- Benutzername und Passwort für ein Konto mit Berechtigung für den Zugriff auf die ONTAP REST API

Schritte

1. Geben Sie die URL in Ihren Browser ein und drücken Sie **Enter**:

   `https://<ip_address>/docs/api`

2. Melden Sie sich über das ONTAP Konto an.

Die Dokumentationsseite für die ONTAP-API wird angezeigt, auf der die API-Aufrufe unten in den Hauptressourcenkategorien organisiert sind.

3. Scrollen Sie als Beispiel für einen einzelnen API-Aufruf in die Kategorie **Cluster** und klicken Sie auf **GET /Cluster**.

Weitere Informationen .

Es stehen verschiedene zusätzliche Ressourcen zur Verfügung, die Sie bei der Automatisierung der Implementierung und Administration Ihrer ONTAP Storage-Systeme unterstützen.

Blog-Artikel

- Eine gute Zusammenfassung der aktuellen Automatisierungstechnologien von ONTAP.

  "Neue Normalität für die Automatisierung"

- Eine Einführung in den Zugriff auf und die Verwendung der Python Samples Skripte bei GitHub für die ONTAP REST API.

  "Erste Schritte mit Beispielskripten bei GitHub"

- Das CLI-Passthrough bietet eine Technik zum Ausführen von ONTAP-CLI-Befehlen unter Verwendung der REST-API.

  "Verwenden des privaten CLI-Passthrough mit der ONTAP REST API"

- Neu bei Ansible zur ONTAP-Automatisierung:

  "Erste Schritte mit NetApp und Ansible – Installation von Ansible"

- Entdecken Sie, wie Sie Dateisicherheit und -Berechtigungen mit der ONTAP REST-API managen.

  "Vereinfachtes Management von Dateisicherheitsberechtigungen mit ONTAP REST-APIs"

- Sie können ONTAP-Ereignisse überwachen, um stets über die Systemaktivität informiert zu bleiben. Die Konfiguration und das Management dieser Ereignisse können mit der REST-API automatisiert werden.

  "ONTAP REST-APIs: Automatische Benachrichtigung über Ereignisse hoher Schweregrad"

- Über die REST-API können Rollen und Zugriffsebenen als Teil einer RBAC-Sicherheitsumgebung konfiguriert werden.

  "Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) mit ONTAP REST-APIs"

- NetApp bietet Python-Beispielskripte zur Verwendung der ONTAP-REST-API.

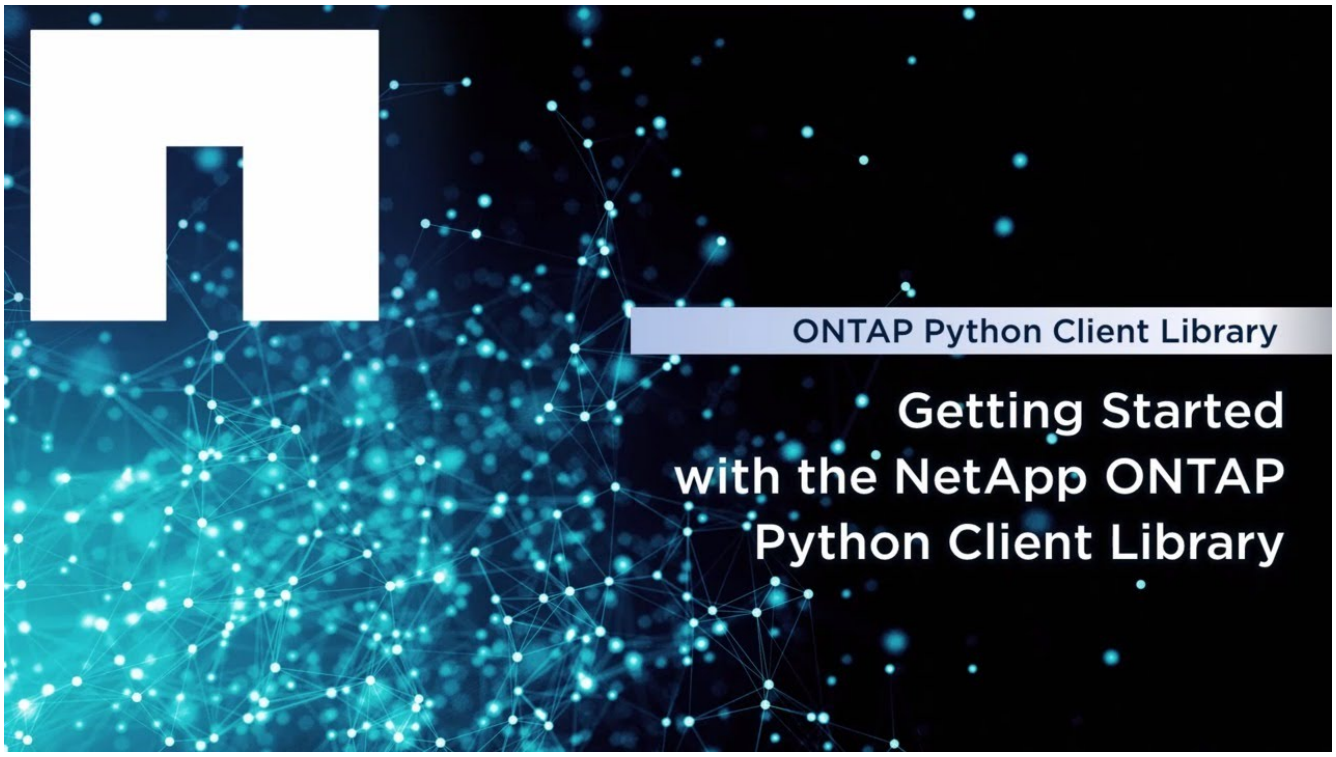
  "ONTAP REST API Python Beispielskripts jetzt auf GitHub verfügbar!"

- Kaffeepausen mit RUHE (6 Episoden).
  - "Grundlagen der ONTAP REST-APIs"
  - "Funktionen von ONTAP REST-APIs"
  - "Praktische Erfahrungen mit ONTAP REST mit Postman"
  - "ONTAPI (ZAPI) Reporting-Tool"
  - "Private CLI-Passthrough"

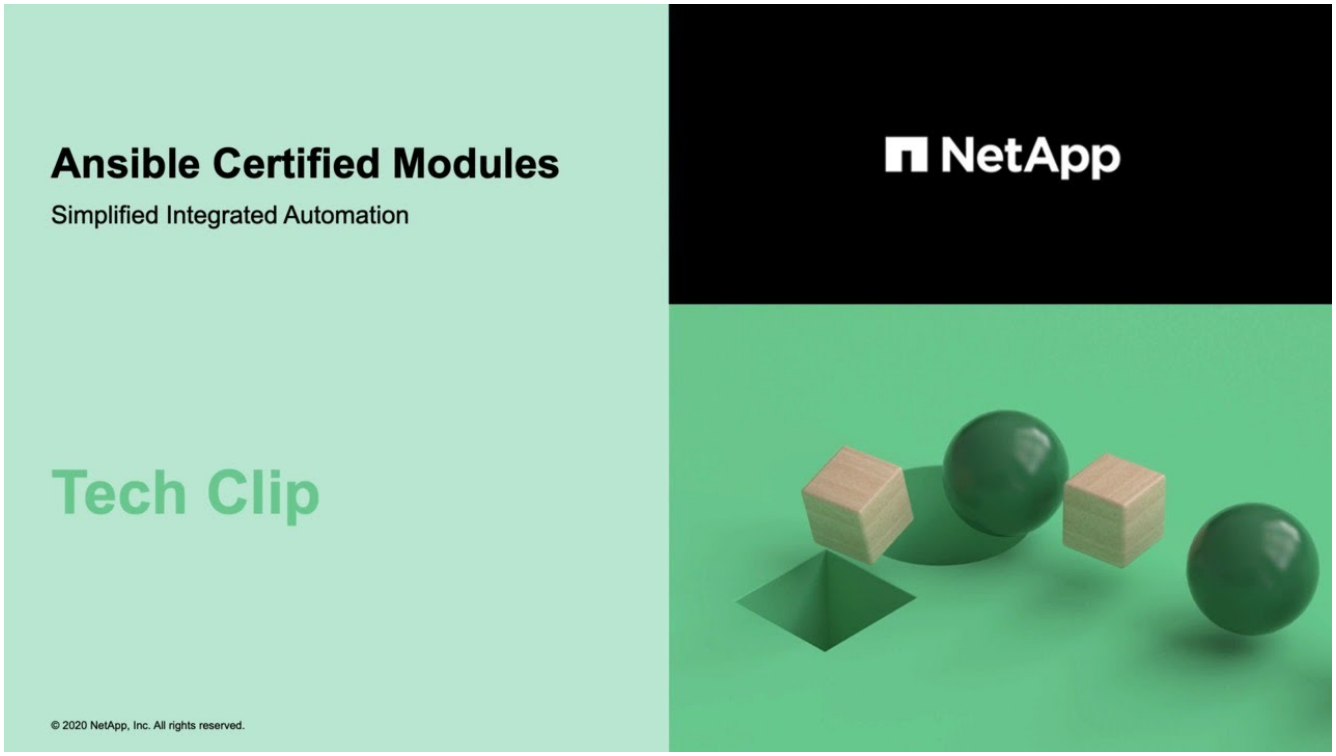
- "5 magische Funktionen, die die ONTAP Storage-Automatisierung vereinfachen!"

Videos

- Eine gute Einführung in die NetApp Python Client Bibliothek und wie man mit dem Schreiben von Code über die Bibliothek beginnt.



- Ansible-zertifizierte Module:



- Eine Sammlung von Videos bei NetApp TechComm TV.

  "Automatisieren Sie das NetApp ONTAP Management"

Technische Schulungen und Veranstaltungen

- Insight 2022-Präsentation (26 Minuten)

  "Modernisieren Sie Ihr ONTAP-Storage-Management mit der ONTAP-REST-API"

- Insight 2021-Präsentation (31 Minuten)

  "NetApp ONTAP: Zeitersparnis und Vereinfachung mit REST-APIs"

- NetApp Learning Services:

  "Automatisieren Sie die Storage-Administration mit der ONTAP REST-API und Ansible"

NetApp Knowledge Base

- Wenn Sie ein Problem mit der ONTAP REST-API haben, können Sie es NetApp melden.

  "So melden Sie Probleme auf der ONTAP REST API und der ONTAP REST API Python Client-Bibliothek"

- Wenn Sie eine funktionale Lücke in der ONTAP-REST-API identifizieren, können Sie eine neue Funktion für die API anfordern.

  "Anfordern einer Funktion für die ONTAP-REST-API"

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

"https://www.netapp.com/company/legal/copyright/"

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"