Workflows

ONTAP automation

NetApp
January 18, 2026

Inhalt

Workflows

Bereiten Sie sich auf die Verwendung der ONTAP REST API-Workflows vor

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

Abrufen der Cluster-Konfiguration mit der ONTAP REST API

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"
}
```

Aktualisieren Sie den Cluster-Kontakt über die ONTAP REST-API

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`.

Abrufen der Job-Instanz mithilfe der ONTAP REST API

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 mithilfe der ONTAP REST API 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"

Erhalten Sie die effektiven Berechtigungen für eine Datei mit der ONTAP REST-API

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"
  ]
}
```


Auditing-Informationen für eine Datei mithilfe der ONTAP REST API

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"
}
```

Anwenden neuer Berechtigungen auf eine Datei mithilfe der ONTAP-REST-API

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`.

Aktualisieren Sie die Security Descriptor-Informationen mithilfe der ONTAP REST API

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 Sie einen Zugriffssteuerungseintrag über die ONTAP-REST-API

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

Führen Sie die IP-Schnittstellen mit der ONTAP REST API 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

Führen Sie die Konten auf, die die ONTAP REST-API verwenden

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

Führen Sie die installierten Zertifikate mithilfe der ONTAP REST API 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 mithilfe der ONTAP REST API

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 der RBAC mithilfe der ONTAP REST API 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 mithilfe der ONTAP-REST-API

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/privileges" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON-Eingabebeispiel

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

Administration der Datensicherung über die ONTAP REST API aktivieren

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"}
  ]
}
```

Ermöglichen Sie die Erstellung von ONTAP-Berichten über die ONTAP-REST-API

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 mithilfe der ONTAP-REST-API

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":"<password>"
}
```

Nachdem Sie fertig sind

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

Storage

Erstellen Sie eine Liste der Aggregate mithilfe der ONTAP REST API

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"
    }
  }
}
```


Führen Sie die Festplatten mit der ONTAP REST API 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

Bereiten Sie sich auf die Verwaltung der EMS-Support-Services mithilfe der ONTAP-REST-API vor

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"

Führen Sie die EMS-Protokollereignisse mithilfe der REST-API von ONTAP 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 mit der ONTAP REST API 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 mithilfe der REST-API von ONTAP

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

Führen Sie eine Liste der SVMs mit der ONTAP REST API 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"
    }
  }
}
```