Flussi di lavoro

ONTAP Automation

NetApp
July 19, 2024

Sommario

Flussi di lavoro

Preparati a utilizzare i flussi di lavoro

È necessario conoscere la struttura e il formato dei flussi di lavoro prima di utilizzarli con una distribuzione ONTAP in tempo reale.

È necessario assicurarsi che la versione ONTAP supporti tutte le chiamate API nei flussi di lavoro che si intende utilizzare. Vedere "Riferimento API" per ulteriori informazioni.

Introduzione

Un *workflow* è una sequenza di uno o più passaggi necessari per eseguire un'attività o un obiettivo amministrativo specifico. I flussi di lavoro di ONTAP includono i passaggi fondamentali e i parametri necessari per eseguire ciascuna attività. Forniscono un punto di partenza per personalizzare il vostro ambiente di automazione ONTAP.

Tipi di passo

Ciascuna fase di un flusso di lavoro ONTAP è di uno dei seguenti tipi:

- REST API Call (con dettagli come ad esempio CURL e JSON)
- Eseguire o richiamare un altro flusso di lavoro ONTAP
- Attività correlate a varie (ad esempio, prendere una decisione di configurazione)

Chiamate API REST

La maggior parte dei passaggi del flusso di lavoro sono chiamate API REST. Questi passaggi utilizzano un formato comune che include un esempio di arricciatura e altre informazioni. Vedere "Riferimento API" Per ulteriori informazioni sulle chiamate API REST.

Flussi di lavoro a fase singola

Un flusso di lavoro può contenere un solo passaggio. Questi *flussi di lavoro a fase singola* sono formattati in modo leggermente diverso rispetto ai flussi di lavoro che contengono più passaggi. Ad esempio, il nome dell'operazione esplicita viene rimosso. L'azione o l'operazione deve essere chiara in base al titolo del flusso di lavoro.

Variabili di input

I flussi di lavoro sono progettati per essere il più generali possibile, pertanto possono essere utilizzati in qualsiasi ambiente ONTAP. Tenendo presente ciò, le chiamate API REST utilizzano variabili negli esempi curl e in altri input. Le chiamate API REST possono quindi essere facilmente adattate a diversi ambienti ONTAP.

Formato URL di base

È possibile accedere all'API REST ONTAP direttamente tramite curl o un linguaggio di programmazione. In questo caso, l'URL di base è diverso dall'URL utilizzato quando si accede alla documentazione online di ONTAP o a Gestione sistema.

Quando si accede direttamente all'API, è necessario aggiungere **api** al dominio o all'indirizzo IP. Ad esempio:

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

Vedere "Come accedere all'API REST di ONTAP" per ulteriori informazioni.

Parametri di input comuni

Esistono diversi parametri di input comunemente utilizzati con la maggior parte delle chiamate API REST. Questi parametri in genere non vengono descritti nei singoli flussi di lavoro. È necessario acquisire familiarità con i parametri. Vedere "Variabili di input che controllano una richiesta API" per ulteriori informazioni.

Se sono necessari parametri aggiuntivi per una specifica chiamata API REST, essi sono inclusi nella sezione **parametri di input aggiuntivi per l'esempio curl** per ogni flusso di lavoro.

Formato variabile

I valori ID e le altre variabili utilizzate con gli esempi di flusso di lavoro sono opachi e possono variare con ogni cluster ONTAP. Per migliorare la leggibilità degli esempi, non vengono utilizzati i valori effettivi. Vengono utilizzate invece le variabili. Questo approccio, basato su un formato coerente e su un insieme di nomi riservati, presenta diversi vantaggi, tra cui:

- I campioni Curl e JSON sono più leggibili e facili da capire.
- Poiché tutte le parole chiave utilizzano lo stesso formato, è possibile identificarle rapidamente.
- Non vi è alcuna esposizione di sicurezza perché i valori non possono essere copiati e riutilizzati.

Le variabili sono formattate per essere usate in un ambiente di shell Bash. Ogni variabile inizia con un simbolo del dollaro ed è racchiusa tra virgolette doppie secondo necessità. Questo li rende riconoscibili per Bash. Il maiuscolo viene utilizzato costantemente per i nomi.

Ecco alcune delle parole chiave variabili più comuni. Questo elenco non è esaustivo e, se necessario, vengono utilizzate variabili aggiuntive. Il loro significato dovrebbe essere ovvio in base al contesto.

Parola chiave	Tipo	Descrizione
$FQDN_IP	URL	Il nome di dominio o l'indirizzo IP pienamente qualificato della LIF di gestione ONTAP.
$CLUSTER_ID	Percorso	Valore UUIDv4 che identifica il cluster ONTAP in cui vengono eseguite le operazioni API.
$BASIC_AUTH	Intestazione	Stringa di credenziali utilizzata per l'autenticazione di base HTTP.

Esempi di input JSON

Alcune delle chiamate API REST, ad esempio quelle che utilizzano POST o PATCH, richiedono l'input JSON nel corpo della richiesta. Gli esempi di input JSON sono presentati separatamente dagli esempi di arricciatura per chiarezza. È possibile utilizzare gli esempi di input JSON con una delle tecniche descritte di seguito.

Salva su file locale

È possibile copiare l'esempio di input JSON in un file e salvarlo localmente. Il comando curl si riferisce al file utilizzando il `--data` parametro con il valore che indica il nome del file con un `@` prefisso.

Incollare nel terminale dopo l'esempio di arricciatura

Per prima cosa è necessario copiare e incollare l'esempio Curl in una shell terminale. Quindi modificare l'esempio per rimuovere completamente `--data` parametro alla fine e sostituirlo con l'attrezzo `--data-raw` parametro. Infine, copiare e incollare nell'esempio JSON in modo che segua il comando curl con il parametro aggiornato. È necessario utilizzare virgolette singole per racchiudere l'esempio di input JSON.

Opzioni di autenticazione

La tecnica di autenticazione principale disponibile per l'API REST è l'autenticazione di base HTTP. A partire da ONTAP 9,14, è inoltre possibile utilizzare il framework Open Authorization (OAuth 2,0) con autenticazione e autorizzazione basate su token.

Autenticazione di base HTTP

Quando si utilizza l'autenticazione di base, le credenziali utente devono essere incluse in ogni richiesta HTTP. Sono disponibili due opzioni per l'invio delle credenziali.

Creare l'intestazione della richiesta HTTP

È possibile creare manualmente l'intestazione Authorization e includerla con le richieste HTTP. Questo può essere fatto quando si usa un comando curl nella CLI o un linguaggio di programmazione con il codice di automazione. I passaggi di alto livello includono:

1. Concatenare i valori dell'utente e della password con due punti:

   ```
   admin:david123
   ```

2. Convertire l'intera stringa in base64:

   ```
   YWRtaW46ZGF2aWQxMjM=
   ```

3. Creare l'intestazione della richiesta:

   ```
   Authorization: Basic YWRtaW46ZGF2aWQxMjM=
   ```

Gli esempi di curl del flusso di lavoro includono questa intestazione con la variabile **$BASIC_AUTH** che è necessario aggiornare prima dell'uso.

Utilizzare un parametro Curl

Un'altra opzione quando si utilizza Curl è rimuovere l'intestazione Authorization e utilizzare invece il parametro curl **user**. Ad esempio:

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

È necessario sostituire le credenziali appropriate per l'ambiente in uso. Le credenziali non sono codificate in base64. Quando si esegue il comando curl con questo parametro, la stringa viene codificata e l'intestazione Authorization viene generata per l'utente.

OAuth 2,0

Quando si utilizza OAuth 2,0, è necessario richiedere un token di accesso da un server di autorizzazione esterno e includerlo in ogni richiesta HTTP. I passaggi di base di alto livello sono descritti di seguito. Vedere anche "Panoramica dell'implementazione di ONTAP OAuth 2,0" Per ulteriori informazioni su OAuth 2,0 e su come utilizzarlo con ONTAP.

Prepara il tuo ambiente ONTAP

Prima di utilizzare l'API REST per accedere a ONTAP, è necessario preparare e configurare l'ambiente ONTAP. Ad un livello elevato, i passaggi includono:

- Identificare le risorse e i client protetti da ONTAP

- Esaminare il ruolo REST ONTAP esistente e le definizioni utente
- Installare e configurare il server di autorizzazione
- Progettare e configurare le definizioni di autorizzazione client
- Configurare ONTAP e attivare OAuth 2,0

Richiedere un token di accesso

Con ONTAP e il server di autorizzazione definiti e attivi, è possibile effettuare una chiamata API REST utilizzando un token OAuth 2,0. Il primo passaggio consiste nel richiedere un token di accesso al server di autorizzazione. Questa operazione viene eseguita al di fuori di ONTAP utilizzando una delle diverse tecniche basate sul server. ONTAP non rilascia token di accesso né esegue il reindirizzamento.

Creare l'intestazione della richiesta HTTP

Dopo aver ottenuto un token di accesso, è possibile creare un'intestazione di autorizzazione e includerla con le richieste HTTP. Indipendentemente dal fatto che si utilizzi curl o un linguaggio di programmazione per accedere all'API REST, è necessario includere l'intestazione con ogni richiesta del client. È possibile costruire l'intestazione come segue:

```
Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSld …
```

Uso degli esempi con Bash

Se si utilizzano direttamente gli esempi di curl del flusso di lavoro, è necessario aggiornare le variabili che contengono con i valori appropriati per l'ambiente in uso. Potete modificare manualmente gli esempi o affidarvi alla shell Bash per eseguire la sostituzione come descritto di seguito.

Un vantaggio dell'utilizzo di Bash è che è possibile impostare i valori delle variabili una volta in una sessione di shell invece di una volta per comando curl.

Fasi

1. Aprire la shell Bash fornita con Linux o un sistema operativo simile.
2. Impostare i valori delle variabili inclusi nell'esempio di arricciatura che si desidera eseguire. Ad esempio:

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

3. Copiare l'esempio di arricciatura dalla pagina del flusso di lavoro e incollarlo nel terminale della shell.
4. Premere **INVIO** per effettuare le seguenti operazioni:
   a. Sostituire i valori della variabile impostati
   b. Eseguire il comando curl

Cluster

Ottenere la configurazione del cluster

È possibile recuperare la configurazione per un cluster ONTAP che include campi specifici. Questa operazione può essere eseguita durante la valutazione dello stato del cluster o prima di aggiornare la configurazione.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/cluster

Parametri di input aggiuntivi per esempi di arricciatura

Oltre ai parametri comuni a tutte le chiamate REST API, nell'esempio curl in questo passo vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
campi	Query	No	Selezionare i valori che si desidera restituire. Alcuni esempi sono `contact` e. `version`.

Esempio Curl: Recupero delle informazioni di contatto del cluster

In questo esempio viene illustrato come recuperare un singolo campo. Per ottenere l'intero oggetto e la configurazione del cluster, è necessario rimuovere l' `fields` parametro di query.

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

Esempio di output JSON

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

Aggiornare il contatto del cluster

È possibile aggiornare le informazioni di contatto per un cluster. Poiché la richiesta viene elaborata in modo asincrono, è necessario anche determinare se il processo in background associato è stato completato correttamente.

Passaggio 1: Aggiornare le informazioni di contatto del quadro strumenti

È possibile eseguire una chiamata API per aggiornare le informazioni di contatto del cluster.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
PATCH	/api/cluster

Tipo di elaborazione

Asincrono

Esempio di arricciamento

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

Esempio di input JSON

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

Esempio di output JSON

Viene restituito un oggetto lavoro. È necessario salvare l'identificatore del lavoro per utilizzarlo nel passo successivo.

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

Passo 2: Recupero dello stato del lavoro

Eseguire il flusso di lavoro "Recupera istanza lavoro" e confermare `state` il valore è `success`.

Fase 3: Confermare le informazioni di contatto del quadro strumenti

Eseguire il flusso di lavoro "Ottenere la configurazione del cluster". Impostare `fields` parametro query a. `contact`.

Recupera istanza lavoro

È possibile recuperare l'istanza di un processo ONTAP specifico. In genere, questa operazione viene eseguita per determinare se il processo e l'operazione associata sono

stati completati correttamente.

È necessario l'UUID dell'oggetto lavoro, che in genere viene fornito dopo l'emissione di una richiesta asincrona. Inoltre, rivedere "Elaborazione asincrona utilizzando l'oggetto Job" Prima di lavorare con i job interni di ONTAP.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/cluster/jobs/{uuid}

Tipo di elaborazione

Sincrono

Parametri di input aggiuntivi per gli esempi Curl

Oltre ai parametri comuni a tutte le chiamate API REST, negli esempi di curl vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
$JOB_ID	Percorso	Sì	Necessario per identificare il lavoro richiesto.

Esempio di arricciamento

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

Esempio di output JSON

Il valore di stato e gli altri campi sono inclusi nell'oggetto lavoro restituito. Il lavoro in questo esempio è stato eseguito come parte dell'aggiornamento di un cluster ONTAP.

```
{
  "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

Permessi di sicurezza del file

Prepararsi a gestire la sicurezza dei file e le policy di controllo

È possibile gestire le autorizzazioni e le policy di audit per i file disponibili nelle SVM all'interno di un cluster ONTAP.

Panoramica

ONTAP utilizza gli elenchi di controllo di accesso di sistema (SACL) e gli elenchi di controllo di accesso discrezionali (DACL) per assegnare le autorizzazioni agli oggetti file. A partire da ONTAP 9,9.1, l'API REST include il supporto per la gestione delle autorizzazioni SACL e DACL. È possibile utilizzare l'API per automatizzare l'amministrazione delle autorizzazioni di protezione dei file. In molti casi è possibile utilizzare una singola chiamata API REST invece di più comandi CLI o chiamate ONTAPI (ZAPI).

> Per le versioni ONTAP precedenti alla 9,9.1, è possibile automatizzare l'amministrazione delle autorizzazioni SACL e DACL utilizzando la funzione Passthrough CLI. Vedere "Considerazioni sulla migrazione" e. "Utilizzo del pass-through CLI privato con l'API REST di ONTAP" per ulteriori informazioni.

Sono disponibili diversi flussi di lavoro di esempio per illustrare come gestire i servizi di sicurezza dei file ONTAP utilizzando l'API REST. Prima di utilizzare i flussi di lavoro e di inviare una qualsiasi delle chiamate API REST, assicurarsi di riesaminarla "Preparati a utilizzare i flussi di lavoro".

Se si utilizza Python, vedere anche lo script "file_security_permissions.py" per esempi su come automatizzare alcune attività di protezione dei file.

API REST ONTAP e comandi CLI ONTAP

Per molte attività, l'utilizzo dell'API REST ONTAP richiede un numero inferiore di chiamate rispetto ai comandi CLI o alle chiamate ONTAPI (ZAPI) di ONTAP equivalenti. La tabella seguente include un elenco di chiamate API e l'equivalente dei comandi CLI necessari per ciascuna attività.

API REST di ONTAP	CLI 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`

Informazioni correlate

- "Script Python che illustra le autorizzazioni dei file"
- "Gestione semplificata delle autorizzazioni di sicurezza dei file con le API REST di ONTAP"
- "Utilizzo del pass-through CLI privato con l'API REST di ONTAP"

Ottenere le autorizzazioni effettive per un file

È possibile recuperare le autorizzazioni effettive correnti per un file o una cartella specifici.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/protocolli/file-security/effective-permissions/{svm.uuid}/{path}

Tipo di elaborazione

Sincrono

Parametri di input aggiuntivi per esempi di arricciatura

Oltre ai parametri comuni a tutte le chiamate REST API, nell'esempio curl in questo passo vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
$SVM_ID	Percorso	Sì	UUUID della SVM che contiene il file.
$PERCORSO_FILE	Percorso	Sì	Questo è il percorso del file o della cartella.

Esempio di arricciamento

```
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"
```

Esempio di output JSON


```
{
  "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"
  ]
}
```


Ottenere le informazioni di controllo per un file

È possibile recuperare le informazioni di controllo per un file o una cartella specifici.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/protocolli/file-security/permissions/{svm.uuid}/{path}

Tipo di elaborazione

Sincrono

Parametri di input aggiuntivi per esempi di arricciatura

Oltre ai parametri comuni a tutte le chiamate REST API, nell'esempio curl in questo passo vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
$SVM_ID	Percorso	Sì	UUUID della SVM che contiene il file.
$PERCORSO_FILE	Percorso	Sì	Questo è il percorso del file o della cartella.

Esempio di arricciamento

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

Esempio di output JSON


```
{
  "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"
}
```

Applicare nuove autorizzazioni a un file

È possibile applicare un nuovo descrittore di protezione a un file o una cartella specifici.

Passaggio 1: Applicare le nuove autorizzazioni

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/protocolli/file-security/permissions/{svm.uuid}/{path}

Tipo di elaborazione

Asincrono

Parametri di input aggiuntivi per esempi di arricciatura

Oltre ai parametri comuni a tutte le chiamate REST API, nell'esempio curl in questo passo vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
$SVM_ID	Percorso	Sì	UUUID della SVM che contiene il file.
$PERCORSO_FILE	Percorso	Sì	Questo è il percorso del file o della cartella.

Esempio di arricciamento

```
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\"}'
```

Esempio di output JSON

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

Passo 2: Recupero dello stato del lavoro

Eseguire il flusso di lavoro "Recupera istanza lavoro" e confermare `state` il valore è `success`.

Aggiornare le informazioni del descrittore di protezione

È possibile aggiornare un descrittore di protezione specifico a un file o una cartella specifici, inclusi i flag del proprietario, del gruppo o del controllo principale.

Passaggio 1: Aggiornare il descrittore di protezione

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
PATCH	/api/protocolli/file-security/permissions/{svm.uuid}/{path}

Tipo di elaborazione

Asincrono

Parametri di input aggiuntivi per esempi di arricciatura

Oltre ai parametri comuni a tutte le chiamate REST API, nell'esempio curl in questo passo vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
$SVM_ID	Percorso	Sì	UUUID della SVM che contiene il file.
$PERCORSO_FILE	Percorso	Sì	Questo è il percorso del file o della cartella.

Esempio di arricciamento

```
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\"}'
```

Esempio di output JSON

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

Passo 2: Recupero dello stato del lavoro

Eseguire il flusso di lavoro "Recupera istanza lavoro" e confermare `state` il valore è `success`.

Eliminare una voce di controllo degli accessi

È possibile eliminare una voce ACE (Access Control Entry) esistente da un file o una cartella specifici. La modifica si propaga a qualsiasi oggetto figlio.

Passaggio 1: Eliminare l'ACE

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
ELIMINARE	/api/protocolli/file-security/permissions/{svm.uuid}/{path}

Tipo di elaborazione

Asincrono

Parametri di input aggiuntivi per esempi di arricciatura

Oltre ai parametri comuni a tutte le chiamate REST API, nell'esempio curl in questo passo vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
$SVM_ID	Percorso	Sì	UUUID della SVM che contiene il file.
$PERCORSO_FILE	Percorso	Sì	Questo è il percorso del file o della cartella.

Esempio di arricciamento

```
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\"}'
```

Esempio di output JSON

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

Passo 2: Recupero dello stato del lavoro

Eseguire il flusso di lavoro "Recupera istanza lavoro" e confermare `state` il valore è `success`.

Networking

List the IP interfaces (Elenca interfacce

È possibile recuperare le LIF IP assegnate al cluster e alle SVM. Questa operazione potrebbe essere utile per confermare la configurazione di rete o per aggiungere un'altra LIF.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/network/ip/interfaces

Tipo di elaborazione

Sincrono

Parametri di input aggiuntivi per gli esempi Curl

Oltre ai parametri comuni a tutte le chiamate API REST, negli esempi di curl vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
campi	Query	No	Restituire un elenco limitato dei valori di configurazione pertinenti.

Esempio di curl: Restituisce tutte le LIF con i valori di configurazione predefiniti

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

Esempio Curl: Restituisce tutte le LIF con quattro valori di configurazione specifici

```
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"
```

Esempio di output JSON


```
{
  "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"
    }
  }
}
```

Sicurezza

Account

Elencare gli account

È possibile recuperare un elenco degli account. Questa operazione può essere eseguita per valutare l'ambiente di protezione o prima di creare un nuovo account.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/security/accounts

Tipo di elaborazione

Sincrono

Esempio di arricciamento

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

Esempio di output JSON


```
{
  "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"
    }
  }
}
```

Certificati e chiavi

Elencare i certificati installati

È possibile elencare i certificati installati nel cluster ONTAP. È possibile eseguire questa operazione per verificare se un determinato certificato è disponibile o per ottenere l'ID di un certificato specifico.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/sicurezza/certificati

Parametri di input aggiuntivi per esempi di arricciatura

Oltre ai parametri comuni a tutte le chiamate REST API, nell'esempio curl in questo passo vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
max_records	Query	No	Specificare il numero di record che si desidera restituire.

Esempio Curl: Restituire tre certificati

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

Esempio di output JSON


```
{
  "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"
    }
  }
}
```

Installare un certificato

Puoi installare un certificato X,509 firmato nel cluster ONTAP. Questa operazione può essere eseguita durante la configurazione di una funzione o di un protocollo ONTAP che richiede un'autenticazione avanzata.

Prima di iniziare

È necessario disporre del certificato che si desidera installare. Assicurarsi inoltre che tutti i certificati intermedi siano installati secondo necessità.

> Prima di utilizzare gli esempi di input JSON riportati di seguito, assicurarsi di aggiornare `public_certificate` con il certificato dell'ambiente.

Passaggio 1: Installazione del certificato

È possibile eseguire una chiamata API per installare il certificato.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/sicurezza/certificati

Esempio Curl: Installare un certificato CA principale a livello di cluster

```
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
```

Esempio di input JSON


```
{
    "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-----"
}
```


Passaggio 2: Verificare che il certificato sia stato installato

Eseguire il flusso di lavoro "Elencare i certificati installati" e verificare che il certificato sia disponibile.

RBAC

Preparati all'utilizzo del RBAC

Puoi utilizzare la funzionalità RBAC di ONTAP in diversi modi a seconda dell'ambiente. In questa sezione vengono presentati alcuni scenari comuni come flussi di lavoro. In ogni caso, l'attenzione è rivolta a uno specifico obiettivo amministrativo e di protezione.

Prima di creare ruoli e assegnare un ruolo a un account utente ONTAP, è necessario prepararsi esaminando i principali requisiti e le opzioni di protezione presentati di seguito. Inoltre, verificare i concetti generali del flusso di lavoro all'indirizzo "Preparati a utilizzare i flussi di lavoro".

Quale versione di ONTAP stai utilizzando?

La release ONTAP determina quali endpoint REST e le funzionalità RBAC sono disponibili.

Identificare le risorse protette e l'ambito

È necessario identificare le risorse o i comandi da proteggere e l'ambito (cluster o SVM).

Quale accesso deve avere l'utente?

Dopo aver identificato le risorse e l'ambito, è necessario determinare il livello di accesso da concedere.

In che modo gli utenti accedono a ONTAP?

L'utente può accedere a ONTAP tramite l'API REST o CLI o entrambi.

Uno dei ruoli integrati è sufficiente o è necessario un ruolo personalizzato?

È più conveniente utilizzare un ruolo integrato esistente, ma è possibile creare un nuovo ruolo personalizzato, se necessario.

Che tipo di ruolo è necessario?

In base ai requisiti di sicurezza e all'accesso a ONTAP, è necessario scegliere se creare un ruolo REST o tradizionale.

Creare ruoli

Limitare l'accesso alle operazioni dei volumi SVM

Puoi definire un ruolo per limitare l'amministrazione del volume storage all'interno di una SVM.

Questo flusso di lavoro

Viene dapprima creato un ruolo tradizionale per consentire inizialmente l'accesso a tutte le principali funzioni di amministrazione dei volumi, ad eccezione del cloning. Il ruolo viene definito con le seguenti caratteristiche:

- È in grado di eseguire tutte le operazioni dei volumi CRUD, tra cui Get, create, Modify ed Delete
- Impossibile creare un clone del volume

È quindi possibile aggiornare il ruolo in base alle esigenze. In questo flusso di lavoro, il ruolo viene modificato nel secondo passaggio per consentire all'utente di creare un clone del volume.

Fase 1: Creare il ruolo

Puoi emettere una chiamata API per creare il ruolo RBAC.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/security/ruoli

Esempio di arricciamento

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

Esempio di input JSON

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

Passaggio 2: Aggiornare il ruolo

È possibile eseguire una chiamata API per aggiornare il ruolo esistente.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/security/ruoli

Parametri di input aggiuntivi per esempi di arricciatura

Oltre ai parametri comuni a tutte le chiamate REST API, nell'esempio curl in questo passo vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
$SVM_ID	Percorso	Sì	UUID della SVM che contiene la definizione del ruolo.
$NOME_RUOLO	Percorso	Sì	Nome del ruolo all'interno della SVM da aggiornare.

Esempio di arricciamento

```
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
```

Esempio di input JSON

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

Attivare l'amministrazione della protezione dei dati

Puoi fornire a un utente funzionalità di protezione dei dati limitate.

Questo flusso di lavoro

Il ruolo tradizionale creato viene definito con le seguenti caratteristiche:

- Possibilità di creare ed eliminare snapshot e aggiornare le relazioni di SnapMirror
- Impossibile creare o modificare oggetti di livello superiore come volumi o SVM

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/security/ruoli

Esempio di arricciamento

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

Esempio di input JSON

```
{
  "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"}
  ]
}
```

Consente la generazione di rapporti ONTAP

È possibile creare un ruolo REST per fornire agli utenti la possibilità di generare report ONTAP.

Questo flusso di lavoro

Il ruolo creato viene definito con le seguenti caratteristiche:

- In grado di recuperare tutte le informazioni relative a capacità e performance (ad esempio volume, qtree, LUN, aggregati, nodo, E relazioni SnapMirror)
- Impossibile creare o modificare oggetti di livello superiore (ad esempio volumi o SVM)

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/security/ruoli

Esempio di arricciamento

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

Esempio di input JSON

```
{
  "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"}
  ]
}
```

Creare un utente con un ruolo

È possibile utilizzare questo flusso di lavoro per creare un utente con un ruolo REST associato.

Questo flusso di lavoro

Questo flusso di lavoro include i passaggi tipici necessari per creare un ruolo REST personalizzato e associarlo a un nuovo account utente. Sia l'utente che il ruolo hanno un ambito SVM e sono associati a un SVM di dati specifico. Alcuni passaggi possono essere opzionali o devono essere modificati a seconda dell'ambiente.

Fase 1: Elenco delle SVM di dati nel cluster

Eseguire la seguente chiamata API REST per elencare le SVM nel cluster. L'UUID e il nome di ciascuna SVM sono forniti nell'output.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/svm/svm

Esempio di arricciamento

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

Al termine

Selezionare la SVM desiderata dall'elenco in cui creare il nuovo utente e il nuovo ruolo.

Fase 2: Elencare gli utenti definiti nella SVM

Eseguire la seguente chiamata API REST per elencare gli utenti definiti nella SVM selezionata. È possibile identificare la SVM attraverso il parametro owner.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/security/accounts

Esempio di arricciamento

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

Al termine

In base agli utenti già definiti nella SVM, scegliere un nome univoco per il nuovo utente.

Fase 3: Elencare i ruoli REST definiti per la SVM

Eseguire la seguente chiamata API REST per elencare i ruoli definiti nella SVM selezionata. È possibile identificare la SVM attraverso il parametro owner.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/security/ruoli

Esempio di arricciamento

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

Al termine

In base ai ruoli già definiti nella SVM, scegliere un nome univoco per il nuovo ruolo.

Passaggio 4: Creare un ruolo REST personalizzato

Eseguire la seguente chiamata API REST per creare un ruolo REST personalizzato nella SVM. Il ruolo inizialmente dispone di un solo privilegio che stabilisce un accesso predefinito di **nessuno** in modo che tutti gli accessi siano negati.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/security/ruoli

Esempio di arricciamento

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

Esempio di input JSON

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

Al termine

Eseguire di nuovo il passaggio 3 per visualizzare il nuovo ruolo. È inoltre possibile visualizzare i ruoli nella CLI di ONTAP.

Passaggio 5: Aggiornare il ruolo aggiungendo ulteriori privilegi

Eseguire la seguente chiamata API REST per modificare il ruolo aggiungendo i privilegi necessari.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/security/roles/{owner.uuid}/{name}/privileges

Parametri di input aggiuntivi per esempi di arricciatura

Oltre ai parametri comuni a tutte le chiamate REST API, nell'esempio curl in questo passo vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
$SVM_ID	Percorso	Sì	L'UUID della SVM che contiene la definizione del ruolo.
$NOME_RUOLO	Percorso	Sì	Nome del ruolo all'interno della SVM da aggiornare.

Esempio di arricciamento

```
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
```

Esempio di input JSON

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

Al termine

Eseguire di nuovo il passaggio 3 per visualizzare il nuovo ruolo. È inoltre possibile visualizzare i ruoli nella CLI di ONTAP.

Passaggio 6: Creare un utente

Eseguire la seguente chiamata API REST per creare un account utente. Il ruolo **dprole1** creato in precedenza

è associato al nuovo utente.

È possibile creare l'utente senza un ruolo. In questo caso, all'utente viene assegnato un ruolo predefinito (uno dei due `admin` oppure `vsadmin`) A seconda che l'utente sia definito con cluster o ambito SVM. Sarà necessario modificare l'utente per assegnare un ruolo diverso.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/security/accounts

Esempio di arricciamento

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

Esempio di input JSON

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

Al termine

È possibile accedere all'interfaccia di gestione SVM utilizzando le credenziali del nuovo utente.

Storage

Elenca gli aggregati

È possibile recuperare un elenco di aggregati nel cluster. Questa operazione può essere eseguita per la valutazione dell'utilizzo e delle prestazioni.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/storage/dischi

Tipo di elaborazione

Sincrono

Parametri di input aggiuntivi per gli esempi Curl

Oltre ai parametri comuni a tutte le chiamate API REST, negli esempi di curl vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
node.name	Query	No	Può essere utilizzato per identificare il nodo a cui è collegato ciascun aggregato.

Esempio di curl: Restituisce tutti gli aggregati con i valori di configurazione predefiniti

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

Esempio Curl: Restituisce tutti gli aggregati con un valore di configurazione specifico

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

Esempio di output JSON


```
{
  "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"
    }
  }
}
```


Elencare i dischi

È possibile recuperare un elenco di dischi nel cluster. Questa operazione può essere eseguita per individuare una o più unità di riserva da utilizzare come parte della creazione di un aggregato.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/storage/dischi

Tipo di elaborazione

Sincrono

Parametri di input aggiuntivi per gli esempi Curl

Oltre ai parametri comuni a tutte le chiamate API REST, negli esempi di curl vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
stato	Query	No	Consentono di identificare i dischi di riserva disponibili per i nuovi aggregati.

Esempio di arricciatura: Restituire tutti i dischi

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

Esempio di arricciatura: Restituire i dischi di ricambio

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

Esempio di output JSON


```
{
  "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"
    }
  }
}
```


Supporto

EMS

Prepararsi a gestire i servizi di assistenza EMS

È possibile configurare l'elaborazione del sistema di gestione degli eventi (EMS, Event Management System) per un cluster ONTAP nonché recuperare i messaggi EMS secondo necessità.

Panoramica

Sono disponibili diversi flussi di lavoro di esempio che illustrano come utilizzare i servizi EMS di ONTAP. Prima di utilizzare i flussi di lavoro e di inviare una qualsiasi delle chiamate API REST, assicurarsi di riesaminarla "Preparati a utilizzare i flussi di lavoro".

Se si utilizza Python, vedere anche lo script "events.py" Per esempi su come automatizzare alcune delle attività correlate all'EMS.

API REST ONTAP e comandi CLI ONTAP

Per molte attività, l'utilizzo dell'API REST ONTAP richiede un numero di chiamate inferiore rispetto ai comandi CLI ONTAP equivalenti. La tabella seguente include un elenco di chiamate API e l'equivalente dei comandi CLI necessari per ciascuna attività.

API REST di ONTAP	CLI ONTAP
OTTENERE /support/ems	`event config show`
INVIA /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>`

Informazioni correlate

- "Script Python che illustra EMS"
- "API REST di ONTAP: Notifica automatica degli eventi ad alta severità"

Elencare gli eventi del registro EMS

È possibile recuperare tutti i messaggi di notifica degli eventi o solo quelli con caratteristiche specifiche.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/support/ems/events

Tipo di elaborazione

Sincrono

Parametri di input aggiuntivi per gli esempi Curl

Oltre ai parametri comuni a tutte le chiamate API REST, negli esempi di curl vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
campi	Query	No	Utilizzato per richiedere campi specifici da includere nella risposta.
max_records	Query	No	Può essere utilizzato per limitare il numero di record restituiti in una singola richiesta.
log_message	Query	No	Consente di cercare un valore di testo specifico e di restituire solo i messaggi corrispondenti.
message.severity	Query	No	Limitare i messaggi restituiti a quelli con un livello di gravità specifico, ad esempio `alert`.

Esempio Curl: Restituisce l'ultimo messaggio e il valore del nome

```
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"
```

Esempio Curl: Consente di restituire un messaggio contenente testo e gravità specifici

```
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"
```

Esempio di output JSON


```
{
  "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"
    }
  }
}
```

Ottenere la configurazione EMS

È possibile recuperare la configurazione EMS corrente per un cluster ONTAP. È possibile eseguire questa operazione prima di aggiornare la configurazione o creare una nuova notifica EMS.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/support/ems

Tipo di elaborazione

Sincrono

Esempio di arricciamento

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

Esempio di output JSON

```
{
  "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"
}
```

Creare una notifica EMS

È possibile utilizzare il seguente flusso di lavoro per creare una nuova destinazione di notifica EMS per ricevere i messaggi di evento selezionati.

Passaggio 1: Configurare le impostazioni di posta elettronica a livello di sistema

È possibile effettuare la seguente chiamata API per configurare le impostazioni e-mail a livello di sistema.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
PATCH	/api/support/ems

Tipo di elaborazione

Sincrono

Parametri di input aggiuntivi per gli esempi Curl

Oltre ai parametri comuni a tutte le chiamate API REST, negli esempi di curl vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
mail_from	Query	Sì	Imposta `from` nel campo dei messaggi e-mail di notifica.
mail_server	Query	Sì	Consente di configurare il server di posta SMTP di destinazione.

Esempio di arricciamento

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

Passo 2: Definizione di un filtro dei messaggi

È possibile effettuare una chiamata API per definire una regola di filtro corrispondente ai messaggi.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/support/ems/filters

Tipo di elaborazione

Sincrono

Parametri di input aggiuntivi per gli esempi Curl

Oltre ai parametri comuni a tutte le chiamate API REST, negli esempi di curl vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
Filtro	Corpo	Sì	Include i valori per la configurazione del filtro.

Esempio di arricciamento

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

Esempio di input JSON

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

Passo 3: Creazione di una destinazione di messaggio

È possibile effettuare una chiamata API per creare una destinazione del messaggio.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/support/ems/destinations

Tipo di elaborazione

Sincrono

Parametri di input aggiuntivi per gli esempi Curl

Oltre ai parametri comuni a tutte le chiamate API REST, negli esempi di curl vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
Configurazione destinazione	Corpo	Sì	Include i valori per la destinazione dell'evento.

Esempio di arricciamento

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

Esempio di input JSON

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

SVM

Elencare le SVM

È possibile elencare le Storage Virtual Machine (SVM) definite all'interno di un cluster ONTAP. Queste operazioni possono essere eseguite per trovare l'identificatore di una SVM specifica o per assicurare l'unicità del nome prima di creare una nuova SVM.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/svm/svm

Esempio di arricciamento

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

Esempio di output JSON


```
{
  "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"
    }
  }
}
```

Informazioni sul copyright

Informazioni sul marchio commerciale