



USA API REST di Swift (obsoleto)

StorageGRID 11.8

NetApp
March 19, 2024

Sommario

- USA API REST di Swift (obsoleto) 1
- USA Swift REST API: Panoramica 1
- Verifica della configurazione delle API REST Swift 4
- Operazioni supportate da Swift REST API 5
- Operazioni API Swift REST di StorageGRID 18
- Operazioni rapide monitorate nei registri di audit 21

USA API REST di Swift (obsoleto)

USA Swift REST API: Panoramica

Le applicazioni client possono utilizzare l'API Swift di OpenStack per interfacciarsi con il sistema StorageGRID.



Il supporto per le applicazioni client Swift è stato obsoleto e verrà rimosso in una release futura.

StorageGRID supporta le seguenti versioni specifiche di Swift e HTTP.

Elemento	Versione
Specifica Swift	OpenStack Swift Object Storage API v1 a novembre 2015
HTTP	1,1 Per ulteriori informazioni su HTTP, vedere HTTP/1.1 (RFC 7230-35). Nota: StorageGRID non supporta la pipelining HTTP/1.1.

Informazioni correlate

["OpenStack: API dello storage a oggetti"](#)

Cronologia del supporto delle API Swift in StorageGRID

È necessario essere a conoscenza delle modifiche apportate al supporto del sistema StorageGRID per l'API DI Swift REST.

Rilasciare	Commenti
11,8	
11,7	Il supporto per le applicazioni client Swift è stato obsoleto e verrà rimosso in una release futura.
11,6	Modifiche editoriali minori.
11,5	Eliminata la debole consistenza. Verrà invece utilizzata la coerenza disponibile.
11,4	Aggiunto supporto per TLS 1.3. Aggiunta descrizione dell'interrelazione tra ILM e coerenza.

Rilasciare	Commenti
11,3	Aggiornate le operazioni PUT object per descrivere l'impatto delle regole ILM che utilizzano il posizionamento sincrono all'acquisizione (le opzioni bilanciate e rigide per il comportamento di Ingest). Aggiunta descrizione delle connessioni client che utilizzano endpoint di bilanciamento del carico o gruppi ad alta disponibilità. Le crittografia TLS 1.1 non sono più supportate.
11,2	Modifiche editoriali minori al documento.
11,1	Aggiunto supporto per l'utilizzo di HTTP per connessioni client Swift ai nodi grid. Aggiornate le definizioni dei valori di coerenza.
11,0	Aggiunto supporto per 1,000 container per ciascun account tenant.
10,3	Aggiornamenti amministrativi e correzioni del documento. Rimosse le sezioni per la configurazione dei certificati server personalizzati.
10,2	Supporto iniziale dell'API Swift da parte del sistema StorageGRID. La versione attualmente supportata è OpenStack Swift Object Storage API v1.

Come StorageGRID implementa l'API di Swift REST

Un'applicazione client può utilizzare le chiamate API DI SWIFT REST per connettersi ai nodi di storage e ai nodi gateway per creare container e memorizzare e recuperare oggetti. Ciò consente alle applicazioni orientate ai servizi sviluppate per OpenStack Swift di connettersi allo storage a oggetti on-premise fornito dal sistema StorageGRID.

Gestione rapida degli oggetti

Una volta acquisiti gli oggetti Swift nel sistema StorageGRID, questi vengono gestiti dalle regole ILM (Information Lifecycle Management) delle policy ILM attive. "[Regole ILM](#)" e "[Policy ILM](#)". Determinare il modo in cui StorageGRID crea e distribuisce le copie dei dati a oggetti e il modo in cui gestisce tali copie nel tempo. Ad esempio, una regola ILM potrebbe essere applicata agli oggetti in specifici contenitori Swift e potrebbe specificare che più copie di oggetti vengono salvate in diversi data center per un certo numero di anni.

Contatta il consulente dei servizi professionali NetApp o l'amministratore di StorageGRID per capire come le regole e le policy ILM della griglia influiranno sugli oggetti del tuo account tenant Swift.

Richieste client in conflitto

Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite". La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client Swift iniziano un'operazione.

Garanzie e controlli di coerenza

Per impostazione predefinita, StorageGRID fornisce coerenza di lettura dopo scrittura per gli oggetti appena creati ed eventuale coerenza per gli aggiornamenti degli oggetti e le operazioni HEAD. Qualsiasi "[OTTIENI](#)" a seguito di un completamento riuscito "[IN PRIMO PIANO](#)" sarà in grado di leggere i dati appena scritti. Le

sovrascritture degli oggetti esistenti, gli aggiornamenti dei metadati e le eliminazioni sono coerenti. Le sovrascritture in genere richiedono secondi o minuti per la propagazione, ma possono richiedere fino a 15 giorni.

StorageGRID consente inoltre di controllare la coerenza in base al container. I valori di coerenza forniscono un equilibrio tra la disponibilità degli oggetti e la coerenza di tali oggetti in diversi nodi e siti di storage, in base alle esigenze dell'applicazione.

Raccomandazioni per l'implementazione di Swift REST API

Seguire questi consigli quando si implementa l'API di Swift REST per l'utilizzo con StorageGRID.

Raccomandazioni per la gestione di oggetti inesistenti

Se l'applicazione verifica regolarmente se un oggetto esiste in un percorso in cui non si prevede che l'oggetto esista effettivamente, è necessario utilizzare la coerenza "disponibile". Ad esempio, è necessario utilizzare la coerenza "disponibile" se l'applicazione esegue un'operazione HEAD in una posizione prima di eseguire un'operazione PUT in quella posizione.

In caso contrario, se l'operazione HEAD non trova l'oggetto, potrebbe essere visualizzato un numero elevato di errori 500 nel server interno se uno o più nodi di storage non sono disponibili.

È possibile impostare la consistenza "disponibile" per ciascun contenitore utilizzando ["INVIO di una richiesta di coerenza del container"](#). È possibile impostare la coerenza "disponibile" per ciascun contenitore utilizzando ["OTTENERE una richiesta di coerenza dei container"](#).

Raccomandazioni per i nomi degli oggetti

Per i container creati in StorageGRID 11.4 o versioni successive, non è più necessario limitare i nomi degli oggetti per soddisfare le Best practice di performance. Ad esempio, è ora possibile utilizzare valori casuali per i primi quattro caratteri dei nomi degli oggetti.

Per i container creati in release precedenti a StorageGRID 11.4, continuare a seguire questi consigli per i nomi degli oggetti:

- Non utilizzare valori casuali come primi quattro caratteri dei nomi degli oggetti. Ciò è in contrasto con la precedente raccomandazione AWS per i prefissi dei nomi. Si consiglia invece di utilizzare prefissi non casuali e non univoci, ad esempio `image`.
- Se si segue la precedente raccomandazione AWS per utilizzare caratteri casuali e univoci nei prefissi dei nomi, è necessario anteporre i nomi degli oggetti con un nome di directory. Ovvero, utilizzare questo formato:

```
mycontainer/mydir/f8e3-image3132.jpg
```

Invece di questo formato:

```
mycontainer/f8e3-image3132.jpg
```

Raccomandazioni per "letture di gamma"

Se il ["opzione globale per comprimere gli oggetti memorizzati"](#) È attivato, le applicazioni client Swift dovrebbero evitare di eseguire operazioni GET Object che specificano la restituzione di un intervallo di byte. Queste operazioni di "lettura dell'intervallo" sono inefficienti perché StorageGRID deve decomprimere efficacemente gli oggetti per accedere ai byte richiesti. LE operazioni GET Object che richiedono un piccolo intervallo di byte da un oggetto molto grande sono particolarmente inefficienti; ad esempio, è molto inefficiente leggere un intervallo di 10 MB da un oggetto compresso da 50 GB.

Se gli intervalli vengono letti da oggetti compressi, le richieste del client possono scadere.



Se è necessario comprimere gli oggetti e l'applicazione client deve utilizzare le letture dell'intervallo, aumentare il timeout di lettura per l'applicazione.

Verifica della configurazione delle API REST Swift

È possibile utilizzare l'interfaccia CLI Swift per verificare la connessione al sistema StorageGRID e verificare la possibilità di leggere e scrivere oggetti.

Prima di iniziare

- Il client della riga di comando Swift è stato scaricato e installato: ["SwiftStack: python-swiftclient"](#)
- Se lo si desidera, è necessario ["creato un endpoint del bilanciamento del carico"](#). In caso contrario, si conosce l'indirizzo IP del nodo di archiviazione a cui si desidera connettersi e il numero di porta da utilizzare. Vedere ["Indirizzi IP e porte per le connessioni client"](#).
- Lo hai fatto ["Creato un account tenant Swift"](#).
- Hai effettuato l'accesso all'account tenant e creato almeno un gruppo e un utente. Vedere ["Creare gruppi per un tenant Swift"](#).



Gli utenti tenant Swift devono disporre dell'autorizzazione al gruppo Administrator per eseguire l'autenticazione nell'API REST Swift.

A proposito di questa attività

Se la protezione non è stata configurata, è necessario aggiungere `--insecure` contrassegnare ciascuno di questi comandi.

Fasi

1. Eseguire una query sull'URL delle informazioni per l'implementazione di StorageGRID Swift:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/info
capabilities
```

Ciò è sufficiente per verificare che l'implementazione di Swift sia funzionale. Per verificare ulteriormente la configurazione dell'account memorizzando un oggetto, continuare con i passaggi aggiuntivi.

2. Inserire un oggetto nel contenitore:

```
touch test_object
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
upload test_container test_object
--object-name test_object
```

3. Ottenere il container per verificare l'oggetto:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
list test_container
```

4. Eliminare l'oggetto:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
delete test_container test_object
```

5. Eliminare il contenitore:

```
swift
-U `<_Tenant_Account_ID:Account_User_Name_>`
-K `<_User_Password_>`
-A `\"https://<_FQDN_ | _IP_>:<_Port_>/auth/v1.0`
delete test_container
```

Operazioni supportate da Swift REST API

Il sistema StorageGRID supporta la maggior parte delle operazioni nell'API Swift di OpenStack. Prima di integrare i client API di Swift REST con StorageGRID, esaminare i dettagli di implementazione per le operazioni di account, container e oggetti.

Operazioni supportate in StorageGRID

Sono supportate le seguenti operazioni API Swift:

- ["Operazioni dell'account"](#)
- ["Operazioni container"](#)
- ["Operazioni a oggetti"](#)

Intestazioni di risposta comuni per tutte le operazioni

Il sistema StorageGRID implementa tutte le intestazioni comuni per le operazioni supportate, come definito dall'API di storage a oggetti Swift v1 di OpenStack.

Informazioni correlate

["OpenStack: API dello storage a oggetti"](#)

Endpoint API Swift supportati

StorageGRID supporta i seguenti endpoint API Swift: URL info, URL auth e URL storage.

URL info

È possibile determinare le funzionalità e i limiti dell'implementazione di Swift di StorageGRID inviando una richiesta GET all'URL di base di Swift con il percorso /info.

```
https://FQDN | Node IP:Swift Port/info/
```

Nella richiesta:

- *FQDN* è il nome di dominio completo.
- *Node IP* È l'indirizzo IP del nodo di storage o del nodo gateway sulla rete StorageGRID.
- *Swift Port* È il numero di porta utilizzato per le connessioni API Swift sul nodo di storage o sul nodo gateway.

Ad esempio, il seguente URL info richiede informazioni a un nodo di storage con l'indirizzo IP 10.99.106.103 e utilizzando la porta 18083.

```
https://10.99.106.103:18083/info/
```

La risposta include le funzionalità dell'implementazione di Swift come dizionario JSON. Uno strumento client può analizzare la risposta JSON per determinare le funzionalità dell'implementazione e utilizzarle come vincoli per le successive operazioni di storage.

L'implementazione StorageGRID di Swift consente l'accesso non autenticato all'URL delle informazioni.

URL di autenticazione

Un client può utilizzare l'URL auth di Swift per l'autenticazione come utente di un account tenant.

```
https://FQDN | Node IP:Swift Port/auth/v1.0/
```


Specificare l'ID account tenant, il nome utente e la password come parametri in X-Auth-User e X-Auth-Key intestazioni delle richieste, come segue:

```
X-Auth-User: Tenant_Account_ID:Username
```

```
X-Auth-Key: Password
```

Nelle intestazioni della richiesta:

- *Tenant_Account_ID* È l'ID account assegnato da StorageGRID al momento della creazione del tenant Swift. Si tratta dello stesso ID account tenant utilizzato nella pagina di accesso di Tenant Manager.
- *Username* È il nome di un utente tenant creato in Tenant Manager. Questo utente deve appartenere a un gruppo che dispone dell'autorizzazione di amministratore Swift. L'utente root del tenant non può essere configurato per utilizzare l'API REST Swift.

Se Identity Federation è abilitato per l'account tenant, fornire il nome utente e la password dell'utente federated dal server LDAP. In alternativa, fornire il nome di dominio dell'utente LDAP. Ad esempio:

```
X-Auth-User: Tenant_Account_ID:Username@Domain_Name
```

- *Password* è la password per l'utente tenant. Le password utente vengono create e gestite in Tenant Manager.

La risposta a una richiesta di autenticazione riuscita restituisce un URL di storage e un token di autenticazione, come segue:

```
X-Storage-Url: https://FQDN | Node_IP:Swift_Port/v1/Tenant_Account_ID
```

```
X-Auth-Token: token
```

```
X-Storage-Token: token
```

Per impostazione predefinita, il token è valido per 24 ore dal momento della generazione.

I token vengono generati per un account tenant specifico. Un token valido per un account non autorizza un utente ad accedere a un altro account.

URL dello storage

Un'applicazione client può eseguire chiamate API SWIFT REST per eseguire operazioni di account, container e oggetti supportate su un nodo gateway o un nodo di storage. Le richieste di storage vengono indirizzate all'URL dello storage restituito nella risposta di autenticazione. La richiesta deve includere anche l'intestazione X-Auth-Token e il valore restituito dalla richiesta auth.

```
https://FQDN | IP:Swift_Port/v1/Tenant_Account_ID
```

```
[/container] [/object]
```

```
X-Auth-Token: token
```

Alcune intestazioni di risposta dello storage che contengono statistiche di utilizzo potrebbero non riflettere numeri precisi per gli oggetti modificati di recente. Potrebbero essere necessari alcuni minuti per visualizzare numeri precisi in queste intestazioni.

Le seguenti intestazioni di risposta per le operazioni di account e container sono esempi di quelle che contengono statistiche di utilizzo:

- X-Account-Bytes-Used
- X-Account-Object-Count
- X-Container-Bytes-Used
- X-Container-Object-Count

Informazioni correlate

["Configurare gli account e le connessioni del tenant"](#)

["Operazioni dell'account"](#)

["Operazioni container"](#)

["Operazioni a oggetti"](#)

Operazioni dell'account

Le seguenti operazioni API Swift vengono eseguite sugli account.

OTTIENI un account

Questa operazione recupera l'elenco di container associato alle statistiche di utilizzo dell'account e dell'account.

È necessario il seguente parametro di richiesta:

- Account

È richiesta la seguente intestazione di richiesta:

- X-Auth-Token

I seguenti parametri di query di richiesta supportati sono facoltativi:

- Delimiter
- End_marker
- Format
- Limit
- Marker
- Prefix

Un'esecuzione riuscita restituisce le seguenti intestazioni con una risposta "HTTP/1,1 204 Nessun contenuto" se l'account viene trovato e non ha contenitori o l'elenco contenitori è vuoto; o una risposta "HTTP/1,1 200 OK" se l'account viene trovato e l'elenco contenitori non è vuoto:

- Accept-Ranges

- Content-Length
- Content-Type
- Date
- X-Account-Bytes-Used
- X-Account-Container-Count
- X-Account-Object-Count
- X-Timestamp
- X-Trans-Id

Conto PRINCIPALE

Questa operazione recupera le informazioni e le statistiche dell'account da un account Swift.

È necessario il seguente parametro di richiesta:

- Account

È richiesta la seguente intestazione di richiesta:

- X-Auth-Token

Un'esecuzione riuscita restituisce le seguenti intestazioni con una risposta "HTTP/1.1 204 No Content":

- Accept-Ranges
- Content-Length
- Date
- X-Account-Bytes-Used
- X-Account-Container-Count
- X-Account-Object-Count
- X-Timestamp
- X-Trans-Id

Informazioni correlate

["Operazioni rapide monitorate nei registri di audit"](#)

Operazioni container

StorageGRID supporta un massimo di 1,000 container per account Swift. Le seguenti operazioni API Swift vengono eseguite sui container.

ELIMINA contenitore

Questa operazione rimuove un container vuoto da un account Swift in un sistema StorageGRID.

Sono richiesti i seguenti parametri di richiesta:

- Account
- Container

È richiesta la seguente intestazione di richiesta:

- X-Auth-Token

Un'esecuzione riuscita restituisce le seguenti intestazioni con una risposta "HTTP/1.1 204 No Content":

- Content-Length
- Content-Type
- Date
- X-Trans-Id

OTTIENI container

Questa operazione recupera l'elenco di oggetti associato al contenitore, insieme alle statistiche e ai metadati del contenitore in un sistema StorageGRID.

Sono richiesti i seguenti parametri di richiesta:

- Account
- Container

È richiesta la seguente intestazione di richiesta:

- X-Auth-Token

I seguenti parametri di query di richiesta supportati sono facoltativi:

- Delimiter
- End_marker
- Format
- Limit
- Marker
- Path
- Prefix

Un'esecuzione riuscita restituisce le seguenti intestazioni con una risposta "HTTP/1.1 200 Success" o "HTTP/1.1 204 No Content":

- Accept-Ranges
- Content-Length
- Content-Type
- Date

- X-Container-Bytes-Used
- X-Container-Object-Count
- X-Timestamp
- X-Trans-Id

CONTENITORE DI TESTA

Questa operazione recupera le statistiche e i metadati dei container da un sistema StorageGRID.

Sono richiesti i seguenti parametri di richiesta:

- Account
- Container

È richiesta la seguente intestazione di richiesta:

- X-Auth-Token

Un'esecuzione riuscita restituisce le seguenti intestazioni con una risposta "HTTP/1.1 204 No Content":

- Accept-Ranges
- Content-Length
- Date
- X-Container-Bytes-Used
- X-Container-Object-Count
- X-Timestamp
- X-Trans-Id

METTI container

Questa operazione crea un container per un account in un sistema StorageGRID.

Sono richiesti i seguenti parametri di richiesta:

- Account
- Container

È richiesta la seguente intestazione di richiesta:

- X-Auth-Token

Un'esecuzione riuscita restituisce le seguenti intestazioni con una risposta "HTTP/1.1 201 created" o "HTTP/1.1 202 accepted" (se il container esiste già in questo account):

- Content-Length
- Date

- X-Timestamp
- X-Trans-Id

Il nome di un container deve essere univoco nello spazio dei nomi StorageGRID. Se il container esiste in un altro account, viene restituita la seguente intestazione: "HTTP/1.1 409 Conflict".

Informazioni correlate

["Monitorare e controllare le operazioni"](#)

Operazioni a oggetti

Le seguenti operazioni API Swift vengono eseguite sugli oggetti. Queste operazioni possono essere monitorate in ["Registro di controllo di StorageGRID"](#).

ELIMINA oggetto

Questa operazione elimina il contenuto e i metadati di un oggetto dal sistema StorageGRID.

Sono richiesti i seguenti parametri di richiesta:

- Account
- Container
- Object

È richiesta la seguente intestazione di richiesta:

- X-Auth-Token

Un'esecuzione corretta restituisce le seguenti intestazioni di risposta con un HTTP/1.1 204 No Content risposta:

- Content-Length
- Content-Type
- Date
- X-Trans-Id

Durante l'elaborazione di una richiesta DI ELIMINAZIONE degli oggetti, StorageGRID tenta di rimuovere immediatamente tutte le copie dell'oggetto da tutte le posizioni memorizzate. Se l'esito è positivo, StorageGRID restituisce immediatamente una risposta al client. Se non è possibile rimuovere tutte le copie entro 30 secondi (ad esempio, perché una posizione è temporaneamente non disponibile), StorageGRID mette in coda le copie per la rimozione e indica che il client è riuscito.

Per ulteriori informazioni, vedere ["Modalità di eliminazione degli oggetti"](#).

OTTIENI oggetto

Questa operazione recupera il contenuto dell'oggetto e recupera i metadati dell'oggetto da un sistema StorageGRID.

Sono richiesti i seguenti parametri di richiesta:

- Account
- Container
- Object

È richiesta la seguente intestazione di richiesta:

- X-Auth-Token

Le seguenti intestazioni di richiesta sono opzionali:

- Accept-Encoding
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since
- Range

Un'esecuzione corretta restituisce le seguenti intestazioni con un HTTP/1.1 200 OK risposta:

- Accept-Ranges
- Content-Disposition, restituito solo se Content-Disposition metadati impostati
- Content-Encoding, restituito solo se Content-Encoding metadati impostati
- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Timestamp
- X-Trans-Id

Oggetto TESTA

Questa operazione recupera i metadati e le proprietà di un oggetto acquisito da un sistema StorageGRID.

Sono richiesti i seguenti parametri di richiesta:

- Account
- Container
- Object

È richiesta la seguente intestazione di richiesta:

- X-Auth-Token

Un'esecuzione corretta restituisce le seguenti intestazioni con una risposta "HTTP/1.1 200 OK":

- Accept-Ranges
- Content-Disposition, restituito solo se Content-Disposition metadati impostati
- Content-Encoding, restituito solo se Content-Encoding metadati impostati
- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Timestamp
- X-Trans-Id

METTI oggetto

Questa operazione crea un nuovo oggetto con dati e metadati oppure sostituisce un oggetto esistente con dati e metadati in un sistema StorageGRID.

StorageGRID supporta oggetti con dimensioni fino a 5 TIB (5,497,558,138,880 byte).



Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite". La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client Swift iniziano un'operazione.

Sono richiesti i seguenti parametri di richiesta:

- Account
- Container
- Object

È richiesta la seguente intestazione di richiesta:

- X-Auth-Token

Le seguenti intestazioni di richiesta sono opzionali:

- Content-Disposition
- Content-Encoding

Non utilizzare chunked Content-Encoding Se la regola ILM applicata a un oggetto filtra gli oggetti in base alle dimensioni e utilizza il posizionamento sincrono all'acquisizione (le opzioni bilanciate o rigide per il comportamento di Ingest).

- Transfer-Encoding

Non utilizzare file compressi o a pezzi `Transfer-Encoding` Se la regola ILM applicata a un oggetto filtra gli oggetti in base alle dimensioni e utilizza il posizionamento sincrono all'acquisizione (le opzioni bilanciate o rigide per il comportamento di Ingest).

- `Content-Length`

Se una regola ILM filtra gli oggetti in base alle dimensioni e utilizza il posizionamento sincrono all'acquisizione, è necessario specificare `Content-Length`.



Se non si seguono queste linee guida per `Content-Encoding`, `Transfer-Encoding`, e `Content-Length`, StorageGRID deve salvare l'oggetto prima di poter determinare la dimensione dell'oggetto e applicare la regola ILM. In altre parole, per impostazione predefinita, StorageGRID deve creare copie temporanee di un oggetto in fase di acquisizione. In altri termini, StorageGRID deve utilizzare l'opzione di doppio commit per il comportamento di Ingest.

Per ulteriori informazioni sul posizionamento sincrono e sulle regole ILM, vedere ["Opzioni di protezione dei dati per l'acquisizione"](#).

- `Content-Type`
- `ETag`
- `X-Object-Meta-<name\>` (metadati correlati agli oggetti)

Se si desidera utilizzare l'opzione **tempo di creazione definito dall'utente** come tempo di riferimento per una regola ILM, è necessario memorizzare il valore in un'intestazione definita dall'utente denominata `X-Object-Meta-Creation-Time`. Ad esempio:

```
X-Object-Meta-Creation-Time: 1443399726
```

Questo campo viene valutato come secondi dal 1° gennaio 1970.

- `X-Storage-Class: reduced_redundancy`

Questa intestazione influisce sul numero di copie di oggetti create da StorageGRID se la regola ILM che corrisponde a un oggetto acquisito specifica un comportamento Ingest di doppio commit o bilanciato.

- **Commit doppio:** Se la regola ILM specifica l'opzione commit doppio per il comportamento di Ingest, StorageGRID crea una singola copia provvisoria quando l'oggetto viene acquisito (commit singolo).
- **Balanced:** Se la regola ILM specifica l'opzione `Balanced`, StorageGRID crea una singola copia provvisoria solo se il sistema non è in grado di eseguire immediatamente tutte le copie specificate nella regola. Se StorageGRID è in grado di eseguire il posizionamento sincrono, questa intestazione non ha alcun effetto.

Il `reduced_redundancy` L'intestazione viene utilizzata al meglio quando la regola ILM corrispondente all'oggetto crea una singola copia replicata. In questo caso, utilizzando `reduced_redundancy` elimina la creazione e l'eliminazione non necessarie di una copia di un oggetto extra per ogni operazione di acquisizione.

Utilizzando il `reduced_redundancy` l'intestazione non è consigliata in altre circostanze perché aumenta il rischio di perdita dei dati dell'oggetto durante l'acquisizione. Ad esempio, è possibile che si

verifichino perdite di dati se la singola copia viene inizialmente memorizzata su un nodo di storage che non riesce prima che si verifichi la valutazione ILM.



Avere una sola copia replicata per qualsiasi periodo di tempo mette i dati a rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, quest'ultimo viene perso in caso di errore o errore significativo di un nodo di storage. Inoltre, durante le procedure di manutenzione, ad esempio gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

Si noti che specificando `reduced_redundancy` influisce solo sul numero di copie create quando un oggetto viene acquisito per la prima volta. Non influisce sul numero di copie dell'oggetto create quando l'oggetto viene valutato dalle policy ILM attive e non comporta l'archiviazione dei dati a livelli inferiori di ridondanza nel sistema StorageGRID.

Un'esecuzione corretta restituisce le seguenti intestazioni con una risposta "HTTP/1.1 201 created":

- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Trans-Id

Richiesta DI OPZIONI

La richiesta DI OPZIONI verifica la disponibilità di un singolo servizio Swift. La richiesta DI OPZIONI viene elaborata dal nodo di storage o dal nodo gateway specificato nell'URL.

Metodo DI OPZIONI

Ad esempio, le applicazioni client possono inviare una richiesta DI OPZIONI alla porta Swift su un nodo di storage, senza fornire credenziali di autenticazione Swift, per determinare se il nodo di storage è disponibile. È possibile utilizzare questa richiesta per il monitoraggio o per consentire ai bilanciatori di carico esterni di identificare quando un nodo di storage è inattivo.

Se utilizzato con l'URL info o l'URL di storage, il metodo OPTIONS restituisce un elenco di verbi supportati per l'URL specificato (ad esempio, HEAD, GET, OPZIONI e PUT). Il metodo DELLE OPZIONI non può essere utilizzato con l'URL auth.

È necessario il seguente parametro di richiesta:

- Account

I seguenti parametri di richiesta sono facoltativi:

- Container
- Object

Un'esecuzione riuscita restituisce le seguenti intestazioni con una risposta "HTTP/1,1 204 Nessun contenuto".

Le OPZIONI richieste all'URL di storage non richiedono l'esistenza della destinazione.

- Allow (Un elenco di verbi supportati per l'URL specificato, ad esempio, HEAD, GET, OPZIONI, E PUT)
- Content-Length
- Content-Type
- Date
- X-Trans-Id

Informazioni correlate

["Endpoint API Swift supportati"](#)

Risposte agli errori alle operazioni API di Swift

Comprendere le possibili risposte agli errori può aiutare a risolvere i problemi delle operazioni.

I seguenti codici di stato HTTP potrebbero essere restituiti quando si verificano errori durante un'operazione:

Nome errore Swift	Stato HTTP
AccountNameTooLong, ContainerNameTooLong, HeaderTooBig, InvalidContainerName, InvalidRequest, InvalidURI, MetadataNameTooLong, MetadataValueTooBig, MissingSecurityHeader, ObjectNameTooLong, TooManyContainers, TooManyMetadataItems, TotalMetadataTooLarge	400 richiesta errata
Accesso negato	403 proibita
ContainerNotEmpty, ContainerAlreadyExists	409 conflitto
InternalError	500 errore interno del server
InvalidRange	416 intervallo richiesto non riscontrabile
MethodNon consentito	405 metodo non consentito
MissingContentLength	411 lunghezza richiesta
Non trovato	404 non trovato
Non soddisfatto	501 non implementato
PrecondizioneFailed	412 precondizione non riuscita
ResourceNotFound	404 non trovato

Nome errore Swift	Stato HTTP
Non autorizzato	401 non autorizzato
UnprocessableEntity	422 entità non elaborabile

Operazioni API Swift REST di StorageGRID

Sono state aggiunte operazioni all'API di Swift REST specifiche per il sistema StorageGRID.

OTTENERE una richiesta di coerenza dei container

"[Valori di coerenza](#)" Fornire un equilibrio tra la disponibilità degli oggetti e la coerenza di tali oggetti nei diversi nodi e siti di storage. La richiesta di coerenza del contenitore GET consente di determinare la coerenza applicata a un determinato contenitore.

Richiesta

Richiedi intestazione HTTP	Descrizione
X-Auth-Token	Specifica il token di autenticazione Swift per l'account da utilizzare per la richiesta.
x-ntap-sg-consistency	Specifica il tipo di richiesta, dove <code>true</code> = OTTENERE la coerenza del container, e. <code>false</code> = GET container (OTTIENI container).
Host	Il nome host a cui viene indirizzata la richiesta.

Esempio di richiesta

```
GET /v1/28544923908243208806/Swift container
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: true
Host: test.com
```

Risposta

Intestazione HTTP di risposta	Descrizione
Data	La data e l'ora della risposta.
Connessione	Se la connessione al server è aperta o chiusa.
ID trasm. X	Identificativo univoco della transazione per la richiesta.

Intestazione HTTP di risposta	Descrizione
Contenuto-lunghezza	La lunghezza del corpo di risposta.
x-ntap-sg-consistency	<p>La consistenza applicata al contenitore. Sono supportati i seguenti valori:</p> <p>All: Tutti i nodi ricevono i dati immediatamente o la richiesta non riesce.</p> <p>Strong-Global: Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti.</p> <p>Strong-Site: Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.</p> <p>Read-after-new-write: (Default) fornisce coerenza lettura dopo scrittura per nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. Consigliato per la maggior parte dei casi.</p> <p>Available: Fornisce una coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono raramente letti o per operazioni HEAD o GET su chiavi che non esistono). Non supportato per i bucket S3 FabricPool.</p>

Esempio di risposta

```

HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
x-ntap-sg-consistency: strong-site

```

INVIO di una richiesta di coerenza del container

La richiesta di coerenza del contenitore PUT consente di specificare la coerenza da applicare alle operazioni eseguite su un contenitore. Per impostazione predefinita, i nuovi contenitori vengono creati utilizzando la coerenza "Read-after-new-write".

Richiesta

Richiedi intestazione HTTP	Descrizione
X-Auth-Token	Il token di autenticazione Swift per l'account da utilizzare per la richiesta.

Richiedi intestazione HTTP	Descrizione
x-ntap-sg-consistency	<p>La coerenza da applicare alle operazioni sul contenitore. Sono supportati i seguenti valori:</p> <p>All: Tutti i nodi ricevono i dati immediatamente o la richiesta non riesce.</p> <p>Strong-Global: Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti.</p> <p>Strong-Site: Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.</p> <p>Read-after-new-write: (Default) fornisce coerenza lettura dopo scrittura per nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. Consigliato per la maggior parte dei casi.</p> <p>Available: Fornisce una coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono raramente letti o per operazioni HEAD o GET su chiavi che non esistono). Non supportato per i bucket S3 FabricPool.</p>
Host	Il nome host a cui viene indirizzata la richiesta.

L'interazione tra coerenza e regole ILM per influire sulla protezione dei dati

Entrambi i tipi di scelta "[valore di coerenza](#)" Inoltre, la regola ILM influisce sulla modalità di protezione degli oggetti. Queste impostazioni possono interagire.

Ad esempio, la coerenza utilizzata durante la memorizzazione di un oggetto influisce sul posizionamento iniziale dei metadati degli oggetti, mentre l' "[comportamento di acquisizione](#)" La selezione per la regola ILM influisce sul posizionamento iniziale delle copie a oggetti. Poiché StorageGRID richiede l'accesso sia ai metadati dell'oggetto che ai relativi dati per soddisfare le richieste del client, la selezione di livelli di protezione corrispondenti per il comportamento di coerenza e acquisizione può offrire una migliore protezione iniziale dei dati e risposte di sistema più prevedibili.

Esempio di interazione tra le regole di coerenza e ILM

Si supponga di disporre di una griglia a due siti con la seguente regola ILM e la seguente coerenza:

- **ILM rule:** Creare due copie di oggetti, una nel sito locale e una in un sito remoto. Viene selezionato il comportamento rigoroso dell'acquisizione.
- **: "Strong-Global" (i metadati degli oggetti vengono immediatamente distribuiti a tutti i siti).

Quando un client memorizza un oggetto nella griglia, StorageGRID esegue entrambe le copie degli oggetti e distribuisce i metadati a entrambi i siti prima di restituire il risultato al client.

L'oggetto è completamente protetto contro la perdita al momento dell'acquisizione del messaggio di successo. Ad esempio, se il sito locale viene perso poco dopo l'acquisizione, le copie dei dati dell'oggetto e dei metadati dell'oggetto rimangono nel sito remoto. L'oggetto è completamente recuperabile.

Se invece si è utilizzata la stessa regola ILM e la coerenza "strong-Site", il client potrebbe ricevere un messaggio di successo dopo la replica dei dati dell'oggetto nel sito remoto ma prima della distribuzione dei metadati dell'oggetto. In questo caso, il livello di protezione dei metadati degli oggetti non corrisponde al livello di protezione dei dati degli oggetti. Se il sito locale viene perso poco dopo l'acquisizione, i metadati dell'oggetto andranno persi. Impossibile recuperare l'oggetto.

L'interrelazione tra coerenza e regole ILM può essere complessa. Contattare NetApp per assistenza.

Esempio di richiesta

```
PUT /v1/28544923908243208806/_Swift_container_  
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29  
x-ntap-sg-consistency: strong-site  
Host: test.com
```

Risposta

Intestazione HTTP di risposta	Descrizione
Date	La data e l'ora della risposta.
Connection	Se la connessione al server è aperta o chiusa.
X-Trans-Id	Identificativo univoco della transazione per la richiesta.
Content-Length	La lunghezza del corpo di risposta.

Esempio di risposta

```
HTTP/1.1 204 No Content  
Date: Sat, 29 Nov 2015 01:02:18 GMT  
Connection: CLOSE  
X-Trans-Id: 1936575373  
Content-Length: 0
```

Operazioni rapide monitorate nei registri di audit

Tutte le operazioni riuscite DI ELIMINAZIONE, GET, HEAD, POST e PUT dello storage vengono monitorate nel registro di controllo di StorageGRID. Errori e richieste di informazioni, autenticazione o OPZIONI non vengono registrati.

Operazioni dell'account

- ["OTTIENI un account"](#)

- "Conto PRINCIPALE"

Operazioni container

- "ELIMINA contenitore"
- "OTTIENI container"
- "CONTENITORE DI TESTA"
- "METTI container"

Operazioni a oggetti

- "ELIMINA oggetto"
- "OTTIENI oggetto"
- "Oggetto TESTA"
- "METTI oggetto"

Informazioni correlate

- "Accedere al file di log di audit"
- "Messaggi di audit di scrittura del client"
- "Messaggi di audit in lettura del client"

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.