Utilizzare l'API REST di Swift

StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/it-it/storagegrid-115/swift/history-of-swift-api-support-in-storagegrid.html on October 03, 2025. Always check docs.netapp.com for the latest.

Sommario

USA Swift . . . 1
Supporto API di OpenStack Swift in StorageGRID . . . 1
Cronologia del supporto delle API Swift in StorageGRID . . . 1
Come StorageGRID implementa l'API di Swift REST . . . 2
Raccomandazioni per l'implementazione dell'API Swift REST . . . 3
Configurazione di account e connessioni tenant . . . 4
Creazione e configurazione di account tenant Swift . . . 4
Come configurare le connessioni client . . . 5
Verifica della connessione nella configurazione dell'API Swift . . . 8
Operazioni supportate da Swift REST API . . . 9
Operazioni supportate in StorageGRID . . . 9
Intestazioni di risposta comuni per tutte le operazioni . . . 9
Endpoint API Swift supportati . . . 10
Operazioni dell'account . . . 12
Operazioni container . . . 13
Operazioni a oggetti . . . 15
Richiesta DI OPZIONI . . . 20
Risposte agli errori alle operazioni API di Swift . . . 21
Operazioni API Swift REST di StorageGRID . . . 22
OTTENERE una richiesta di coerenza dei container . . . 22
INVIO di una richiesta di coerenza del container . . . 23
Configurazione della sicurezza per l'API REST . . . 26
In che modo StorageGRID fornisce la sicurezza per l'API REST . . . 26
Algoritmi di hashing e crittografia supportati per le librerie TLS . . . 28
Operazioni di monitoraggio e controllo . . . 29
Monitoraggio delle velocità di acquisizione e recupero degli oggetti . . . 29
Accesso e revisione dei registri di audit . . . 31

USA Swift

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

- "Supporto API di OpenStack Swift in StorageGRID"
- "Configurazione di account e connessioni tenant"
- "Operazioni supportate da Swift REST API"
- "Operazioni API Swift REST di StorageGRID"
- "Configurazione della sicurezza per l'API REST"
- "Operazioni di monitoraggio e controllo"

Supporto API di OpenStack Swift in StorageGRID

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
11.5	Rimosso il controllo di coerenza debole. Verrà invece utilizzato il livello di coerenza disponibile.
11.4	Aggiunto supporto per TLS 1.3 e elenco aggiornato delle suite di crittografia TLS supportate. CLB è obsoleto. Aggiunta descrizione dell'interrelazione tra ILM e l'impostazione di 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. Elenco aggiornato delle suite di crittografia TLS supportate. 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 controlli 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) nella policy ILM attiva del sistema. Le regole e i criteri ILM determinano il modo in cui StorageGRID crea e distribuisce le copie dei dati a oggetti e il modo in cui queste vengono gestite 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.

Contattare l'amministratore di StorageGRID per informazioni su come le regole e le policy ILM della griglia influiranno sugli oggetti dell'account tenant Swift.

Richieste client in conflitto

Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base alle “ultime vittorie”. La tempistica per la valutazione “ultimi successi” si basa su quando il sistema StorageGRID completa una data richiesta e non su quando 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 GET che segue UN PUT completato con successo 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. È possibile modificare il controllo di coerenza per creare un compromesso tra la disponibilità degli oggetti e la coerenza di tali oggetti nei diversi nodi e siti di storage, come richiesto dall’applicazione.

Informazioni correlate

"Gestire gli oggetti con ILM"

"OTTENERE una richiesta di coerenza dei container"

"INVIO di una richiesta di coerenza del container"

Raccomandazioni per l’implementazione dell’API Swift REST

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 l’esistenza di un oggetto in un percorso in cui non si prevede l’effettiva esistenza dell’oggetto, utilizzare il controllo di coerenza “Available”. Ad esempio, è necessario utilizzare il controllo di coerenza “Available” se l’applicazione esegue un’operazione HEAD in una posizione prima di eseguire un’operazione PUT in tale 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 il controllo di coerenza “Available” per ciascun container utilizzando la richiesta DI coerenza PUT container.

Raccomandazioni per i nomi degli oggetti

Non utilizzare valori casuali come primi quattro caratteri dei nomi degli oggetti. Si consiglia invece di utilizzare prefissi non casuali e non univoci, ad esempio image.

Se è necessario utilizzare caratteri casuali e univoci nei prefissi dei nomi degli oggetti, è necessario anteporre i nomi degli oggetti a un nome di directory. Ovvero, utilizzare questo formato:

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

Invece di questo formato:

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

Raccomandazioni per "range reads"

Se l'opzione **compress stored objects** è selezionata (**Configuration** > **System Settings** > **Grid Options**), le applicazioni client Swift dovrebbero evitare di eseguire operazioni GET object che specificano la restituzione di un intervallo di byte. Queste operazioni "range Read" 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.

Informazioni correlate

"OTTENERE una richiesta di coerenza dei container"

"INVIO di una richiesta di coerenza del container"

"Amministrare StorageGRID"

Configurazione di account e connessioni tenant

La configurazione di StorageGRID per accettare connessioni da applicazioni client richiede la creazione di uno o più account tenant e la configurazione delle connessioni.

Creazione e configurazione di account tenant Swift

È necessario un account tenant Swift prima che i client API Swift possano memorizzare e recuperare oggetti su StorageGRID. Ogni account tenant dispone di un proprio ID account, di gruppi e utenti, nonché di container e oggetti.

Gli account del tenant Swift vengono creati da un amministratore del grid StorageGRID utilizzando il grid manager o l'API di gestione del grid.

Quando si crea un account tenant Swift, l'amministratore della griglia specifica le seguenti informazioni:

- Nome visualizzato per il tenant (l'ID account del tenant viene assegnato automaticamente e non può essere modificato)
- Facoltativamente, una quota di storage per l'account tenant, ovvero il numero massimo di gigabyte, terabyte o petabyte disponibili per gli oggetti del tenant. La quota di storage di un tenant rappresenta una quantità logica (dimensione dell'oggetto), non una quantità fisica (dimensione sul disco).
- Se l'SSO (Single Sign-on) non è in uso per il sistema StorageGRID, se l'account tenant utilizzerà la propria origine di identità o condividerà l'origine di identità della griglia e la password iniziale per l'utente root locale del tenant.

- Se SSO è attivato, quale gruppo federato dispone dell'autorizzazione di accesso root per configurare l'account tenant.

Una volta creato un account tenant Swift, gli utenti con l'autorizzazione Root Access possono accedere a Tenant Manager per eseguire attività come le seguenti:

- Impostazione della federazione delle identità (a meno che l'origine delle identità non sia condivisa con la griglia) e creazione di gruppi e utenti locali
- Monitoraggio dell'utilizzo dello storage

> Gli utenti Swift devono disporre dell'autorizzazione Root Access per accedere a Tenant Manager. Tuttavia, l'autorizzazione Root Access non consente agli utenti di autenticarsi nell'API SWIFT REST per creare container e acquisire oggetti. Gli utenti devono disporre dell'autorizzazione di amministratore Swift per autenticarsi nell'API DI Swift REST.

Informazioni correlate

"Amministrare StorageGRID"

"Utilizzare un account tenant"

"Endpoint API Swift supportati"

Come configurare le connessioni client

Un amministratore di grid effettua scelte di configurazione che influiscono sul modo in cui i client Swift si connettono a StorageGRID per memorizzare e recuperare i dati. Le informazioni specifiche necessarie per effettuare una connessione dipendono dalla configurazione scelta.

Le applicazioni client possono memorizzare o recuperare oggetti connettendosi a una delle seguenti opzioni:

- Il servizio Load Balancer sui nodi Admin o Gateway o, facoltativamente, l'indirizzo IP virtuale di un gruppo ad alta disponibilità (ha) di nodi Admin o nodi Gateway
- Il servizio CLB sui nodi gateway o, facoltativamente, l'indirizzo IP virtuale di un gruppo ad alta disponibilità di nodi gateway

> Il servizio CLB è obsoleto. I client configurati prima della release StorageGRID 11.3 possono continuare a utilizzare il servizio CLB sui nodi gateway. Tutte le altre applicazioni client che dipendono da StorageGRID per fornire il bilanciamento del carico devono connettersi utilizzando il servizio bilanciamento del carico.

- Nodi di storage, con o senza bilanciamento del carico esterno

Durante la configurazione di StorageGRID, un amministratore della griglia può utilizzare il gestore della griglia o l'API di gestione della griglia per eseguire le seguenti operazioni, tutte facoltative:

1. Configurare gli endpoint per il servizio Load Balancer.

   È necessario configurare gli endpoint per utilizzare il servizio Load Balancer. Il servizio Load Balancer sui nodi di amministrazione o gateway distribuisce le connessioni di rete in entrata dalle applicazioni client ai nodi di storage. Quando si crea un endpoint di bilanciamento del carico, l'amministratore di StorageGRID specifica un numero di porta, se l'endpoint accetta connessioni HTTP o HTTPS, il tipo di client (S3 o Swift) che utilizzerà l'endpoint e il certificato da utilizzare per le connessioni HTTPS (se applicabile).

2. Configurare reti client non attendibili.

   Se un amministratore di StorageGRID configura una rete client di un nodo come non attendibile, il nodo accetta solo connessioni in entrata sulla rete client su porte esplicitamente configurate come endpoint del bilanciamento del carico.

3. Configurare i gruppi ad alta disponibilità.

   Se un amministratore crea un gruppo ha, le interfacce di rete di più nodi Admin o nodi Gateway vengono inserite in una configurazione di backup attivo. Le connessioni client vengono effettuate utilizzando l'indirizzo IP virtuale del gruppo ha.

Per ulteriori informazioni su ciascuna opzione, consultare le istruzioni per l'amministrazione di StorageGRID.

Riepilogo: Indirizzi IP e porte per le connessioni client

Le applicazioni client si connettono a StorageGRID utilizzando l'indirizzo IP di un nodo Grid e il numero di porta di un servizio su tale nodo. Se sono configurati gruppi ad alta disponibilità (ha), le applicazioni client possono connettersi utilizzando l'indirizzo IP virtuale del gruppo ha.

Informazioni necessarie per stabilire connessioni client

La tabella riassume i diversi modi in cui i client possono connettersi a StorageGRID e gli indirizzi IP e le porte utilizzati per ciascun tipo di connessione. Per ulteriori informazioni, contattare l'amministratore di StorageGRID oppure consultare le istruzioni per l'amministrazione di StorageGRID per una descrizione di come trovare queste informazioni in Gestione griglia.

Dove viene stabilita la connessione	Servizio a cui si connette il client	Indirizzo IP	Porta
Gruppo HA	Bilanciamento del carico	Indirizzo IP virtuale di un gruppo ha	• Porta endpoint del bilanciamento del carico
Gruppo HA	CLB **Nota:** il servizio CLB è obsoleto.	Indirizzo IP virtuale di un gruppo ha	Porte Swift predefinite: • HTTPS: 8083 • HTTP: 8085
Nodo Admin	Bilanciamento del carico	Indirizzo IP del nodo di amministrazione	• Porta endpoint del bilanciamento del carico
Nodo gateway	Bilanciamento del carico	Indirizzo IP del nodo gateway	• Porta endpoint del bilanciamento del carico

Dove viene stabilita la connessione	Servizio a cui si connette il client	Indirizzo IP	Porta
Nodo gateway	CLB **Nota:** il servizio CLB è obsoleto.	Indirizzo IP del nodo gateway **Nota:** per impostazione predefinita, le porte HTTP per CLB e LDR non sono attivate.	Porte Swift predefinite: • HTTPS: 8083 • HTTP: 8085
Nodo di storage	LDR	Indirizzo IP del nodo di storage	Porte Swift predefinite: • HTTPS: 18083 • HTTP: 18085

Esempio

Per connettere un client Swift all'endpoint Load Balancer di un gruppo ha di nodi gateway, utilizzare un URL strutturato come mostrato di seguito:

- `https://VIP-of-HA-group:LB-endpoint-port`

Ad esempio, se l'indirizzo IP virtuale del gruppo ha è 192.0.2.6 e il numero di porta di un endpoint di bilanciamento del carico di Swift è 10444, un client Swift potrebbe utilizzare il seguente URL per connettersi a StorageGRID:

- `https://192.0.2.6:10444`

È possibile configurare un nome DNS per l'indirizzo IP utilizzato dai client per la connessione a StorageGRID. Contattare l'amministratore di rete locale.

Scelta dell'utilizzo di connessioni HTTPS o HTTP

Quando le connessioni client vengono eseguite utilizzando un endpoint Load Balancer, le connessioni devono essere effettuate utilizzando il protocollo (HTTP o HTTPS) specificato per tale endpoint. Per utilizzare HTTP per le connessioni client ai nodi di storage o al servizio CLB sui nodi gateway, è necessario abilitarne l'utilizzo.

Per impostazione predefinita, quando le applicazioni client si connettono ai nodi di storage o al servizio CLB sui nodi gateway, devono utilizzare HTTPS crittografato per tutte le connessioni. In alternativa, è possibile attivare connessioni HTTP meno sicure selezionando l'opzione **Enable HTTP Connection** grid (attiva connessione HTTP) in Grid Manager. Ad esempio, un'applicazione client potrebbe utilizzare il protocollo HTTP quando si verifica la connessione a un nodo di storage in un ambiente non di produzione.

> Prestare attenzione quando si attiva HTTP per una griglia di produzione, poiché le richieste verranno inviate senza crittografia.

> Il servizio CLB è obsoleto.

Se l'opzione **Enable HTTP Connection** (attiva connessione HTTP) è selezionata, i client devono utilizzare porte diverse per HTTP rispetto a quelle utilizzate per HTTPS. Consultare le istruzioni per l'amministrazione di StorageGRID.

Informazioni correlate

"Amministrare StorageGRID"

Verifica della connessione nella configurazione dell'API Swift

È possibile utilizzare l'interfaccia utente di Swift per verificare la connessione al sistema StorageGRID e per verificare che sia possibile leggere e scrivere oggetti nel sistema.

Di cosa hai bisogno

- Devi aver scaricato e installato python-swiftclient, il client della riga di comando di Swift.
- È necessario disporre di un account tenant Swift nel sistema StorageGRID.

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
```

Informazioni correlate

"Creazione e configurazione di account tenant Swift"

"Configurazione della sicurezza per l'API REST"

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

"Come configurare le connessioni client"

"Creazione e configurazione di account tenant Swift"

"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 No Content" se l'account viene trovato e non ha contenitori o l'elenco container è vuoto; oppure una risposta "HTTP/1.1 200 OK" se l'account viene trovato e l'elenco container 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

"Operazioni rapide monitorate nei registri di audit"

Operazioni a oggetti

Le seguenti operazioni API Swift vengono eseguite sugli oggetti.

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 non è temporaneamente disponibile), StorageGRID mette in coda le copie per la rimozione e indica che il client è riuscito.

Per ulteriori informazioni sull'eliminazione degli oggetti, vedere le istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

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 di dimensioni fino a 5 TB.

> Le richieste dei client in conflitto, ad esempio due client che scrivono sulla stessa chiave, vengono risolte in base alle “ultime vittorie”. La tempistica per la valutazione “ultimi successi” si basa su quando il sistema StorageGRID completa una data richiesta e non su quando 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 le istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

- `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 eseguite quando l'oggetto viene valutato dal criterio ILM attivo 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`

Informazioni correlate

"Gestire gli oggetti con ILM"

"Operazioni rapide monitorate nei registri di audit"

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 No Content". 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
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

Il livello di coerenza crea un compromesso tra la disponibilità degli oggetti e la coerenza di tali oggetti nei diversi nodi e siti di storage. La richiesta DI coerenza GET Container consente di determinare il livello di coerenza applicato a un determinato container.

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 `true` = OTTENERE la coerenza del container, e. `false` = 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
`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.

Intestazione HTTP di risposta	Descrizione
`x-ntap-sg-consistency`	Il livello di controllo della coerenza applicato al container. Sono supportati i seguenti valori: • **All**: Tutti i nodi ricevono i dati immediatamente o la richiesta non riesce. • **Strong-Global**: Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti. • **Strong-Site**: Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito. • **Read-after-new-write**: Fornisce coerenza di lettura dopo scrittura per nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. **Nota**: Se l'applicazione utilizza richieste HEAD su oggetti che non esistono, potrebbe essere visualizzato un numero elevato di errori 500 interni del server se uno o più nodi di storage non sono disponibili. Per evitare questi errori, utilizzare il livello "Available". • **Available** (eventuale coerenza per le operazioni HEAD): Si comporta come il livello di coerenza "read-after-new-write", ma fornisce solo una coerenza finale per le operazioni HEAD. Offre una maggiore disponibilità per le operazioni HEAD rispetto a "read-after-new-write" se i nodi storage non sono disponibili.

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
```

Informazioni correlate

"Utilizzare un account tenant"

INVIO di una richiesta di coerenza del container

La richiesta DI coerenza PUT container consente di specificare il livello di coerenza da applicare alle

operazioni eseguite su un container. Per impostazione predefinita, i nuovi contenitori vengono creati utilizzando il livello di 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.
`x-ntap-sg-consistency`	Il livello di controllo della coerenza da applicare alle operazioni sul container. Sono supportati i seguenti valori: • **All**: Tutti i nodi ricevono i dati immediatamente o la richiesta non riesce. • **Strong-Global**: Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti. • **Strong-Site**: Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all’interno di un sito. • **Read-after-new-write**: Fornisce coerenza di lettura dopo scrittura per nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. **Nota**: Se l’applicazione utilizza richieste HEAD su oggetti che non esistono, potrebbe essere visualizzato un numero elevato di errori 500 interni del server se uno o più nodi di storage non sono disponibili. Per evitare questi errori, utilizzare il livello “Available”. • **Available** (eventuale coerenza per le operazioni HEAD): Si comporta come il livello di coerenza “read-after-new-write”, ma fornisce solo una coerenza finale per le operazioni HEAD. Offre una maggiore disponibilità per le operazioni HEAD rispetto a “read-after-new-write” se i nodi storage non sono disponibili.
`Host`	Il nome host a cui viene indirizzata la richiesta.

Come interagiscono i controlli di coerenza e le regole ILM per influire sulla protezione dei dati

La scelta del controllo di coerenza e la regola ILM influiscono sulla modalità di protezione degli oggetti. Queste impostazioni possono interagire.

Ad esempio, il controllo di coerenza utilizzato quando un oggetto viene memorizzato influisce sul

posizionamento iniziale dei metadati dell'oggetto, mentre il comportamento di acquisizione selezionato per la regola ILM influisce sul posizionamento iniziale delle copie dell'oggetto. Poiché StorageGRID richiede l'accesso sia ai metadati di un oggetto che ai suoi dati per soddisfare le richieste dei client, la selezione dei livelli di protezione corrispondenti per il livello di coerenza e il comportamento di acquisizione può fornire una migliore protezione iniziale dei dati e risposte di sistema più prevedibili.

Per le regole ILM sono disponibili i seguenti comportamenti di acquisizione:

- **Strict**: Tutte le copie specificate nella regola ILM devono essere eseguite prima che il client sia riuscito.
- **Balanced**: StorageGRID tenta di eseguire tutte le copie specificate nella regola ILM al momento dell'acquisizione; se ciò non è possibile, vengono eseguite copie temporanee e viene restituito il successo al client. Le copie specificate nella regola ILM vengono eseguite quando possibile.
- **Doppio commit**: StorageGRID esegue immediatamente copie temporanee dell'oggetto e restituisce il successo al client. Le copie specificate nella regola ILM vengono eseguite quando possibile.

> Prima di selezionare il comportamento di acquisizione per una regola ILM, leggere la descrizione completa di queste impostazioni nelle istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

Esempio di come il controllo di coerenza e la regola ILM possono interagire

Si supponga di disporre di una griglia a due siti con la seguente regola ILM e la seguente impostazione del livello di 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.
- **Livello di coerenza**: "strong-Global" (i metadati degli oggetti vengono distribuiti immediatamente 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 sono state utilizzate la stessa regola ILM e il livello di 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'interconnessione tra i livelli di coerenza e le 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
```

Informazioni correlate

"Utilizzare un account tenant"

Configurazione della sicurezza per l'API REST

È necessario esaminare le misure di sicurezza implementate per L'API REST e comprendere come proteggere il sistema.

In che modo StorageGRID fornisce la sicurezza per l'API REST

È necessario comprendere in che modo il sistema StorageGRID implementa la sicurezza, l'autenticazione e l'autorizzazione per l'API REST.

StorageGRID utilizza le seguenti misure di sicurezza.

- Le comunicazioni del client con il servizio Load Balancer utilizzano HTTPS se HTTPS è configurato per l'endpoint del bilanciamento del carico.

  Quando si configura un endpoint di bilanciamento del carico, è possibile attivare HTTP. Ad esempio, è possibile utilizzare HTTP per test o altri scopi non di produzione. Per ulteriori informazioni, consultare le istruzioni per l'amministrazione di StorageGRID.

- Per impostazione predefinita, StorageGRID utilizza HTTPS per le comunicazioni client con i nodi di storage e il servizio CLB sui nodi gateway.

  È possibile abilitare HTTP per queste connessioni. Ad esempio, è possibile utilizzare HTTP per test o altri scopi non di produzione. Per ulteriori informazioni, consultare le istruzioni per l'amministrazione di

StorageGRID.

Il servizio CLB è obsoleto.

- Le comunicazioni tra StorageGRID e il client vengono crittografate mediante TLS.
- Le comunicazioni tra il servizio Load Balancer e i nodi di storage all'interno della griglia vengono crittografate indipendentemente dal fatto che l'endpoint del bilanciamento del carico sia configurato per accettare connessioni HTTP o HTTPS.
- I client devono fornire le intestazioni di autenticazione HTTP a StorageGRID per eseguire operazioni REST API.

Certificati di sicurezza e applicazioni client

I client possono connettersi al servizio Load Balancer sui nodi Gateway o sui nodi Admin, direttamente ai nodi Storage o al servizio CLB sui nodi Gateway.

In tutti i casi, le applicazioni client possono stabilire connessioni TLS utilizzando un certificato server personalizzato caricato dall'amministratore della griglia o un certificato generato dal sistema StorageGRID:

- Quando le applicazioni client si connettono al servizio Load Balancer, utilizzano il certificato configurato per l'endpoint specifico del bilanciamento del carico utilizzato per stabilire la connessione. Ogni endpoint dispone di un proprio certificato, ovvero un certificato server personalizzato caricato dall'amministratore della griglia o un certificato generato dall'amministratore della griglia in StorageGRID durante la configurazione dell'endpoint.
- Quando le applicazioni client si connettono direttamente a un nodo di storage o al servizio CLB sui nodi gateway, utilizzano i certificati server generati dal sistema e generati per i nodi di storage al momento dell'installazione del sistema StorageGRID (firmati dall'autorità di certificazione del sistema), oppure un singolo certificato server personalizzato fornito per la griglia da un amministratore della griglia.

I client devono essere configurati in modo da considerare attendibile l'autorità di certificazione che ha firmato il certificato utilizzato per stabilire connessioni TLS.

Consultare le istruzioni per l'amministrazione di StorageGRID per informazioni sulla configurazione degli endpoint del bilanciamento del carico e per istruzioni sull'aggiunta di un singolo certificato server personalizzato per le connessioni TLS direttamente ai nodi di storage o al servizio CLB sui nodi gateway.

Riepilogo

La seguente tabella mostra come vengono implementati i problemi di sicurezza nelle API S3 e Swift REST:

Problema di sicurezza	Implementazione per API REST
Sicurezza della connessione	TLS
Autenticazione del server	Certificato server X.509 firmato dalla CA di sistema o certificato server personalizzato fornito dall'amministratore
Autenticazione del client	• S3: Account S3 (ID chiave di accesso e chiave di accesso segreta) • Swift: Account Swift (nome utente e password)

Problema di sicurezza	Implementazione per API REST
Autorizzazione del client	• S3: Proprietà del bucket e tutte le policy di controllo degli accessi applicabili • Swift: Accesso al ruolo di amministratore

Informazioni correlate

"Amministrare StorageGRID"

Algoritmi di hashing e crittografia supportati per le librerie TLS

Il sistema StorageGRID supporta un set limitato di suite di crittografia che le applicazioni client possono utilizzare quando si stabilisce una sessione TLS (Transport Layer Security).

Versioni supportate di TLS

StorageGRID supporta TLS 1.2 e TLS 1.3.

SSLv3 e TLS 1.1 (o versioni precedenti) non sono più supportati.

Suite di crittografia supportate

Versione TLS	IANA nome della suite di crittografia
1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1.3	TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256	TLS_AES_128_GCM_SHA256

Suite di crittografia obsolete

Le seguenti suite di crittografia sono obsolete. Il supporto per questi cifrari verrà rimosso in una release futura.

Nome IANA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

Informazioni correlate

"Come configurare le connessioni client"

Operazioni di monitoraggio e controllo

È possibile monitorare i carichi di lavoro e le efficienze per le operazioni dei client visualizzando le tendenze delle transazioni per l'intero grid o per nodi specifici. È possibile utilizzare i messaggi di audit per monitorare le operazioni e le transazioni dei client.

Monitoraggio delle velocità di acquisizione e recupero degli oggetti

È possibile monitorare i tassi di acquisizione e recupero degli oggetti, nonché le metriche per i conteggi degli oggetti, le query e la verifica. È possibile visualizzare il numero di tentativi riusciti e non riusciti da parte delle applicazioni client di lettura, scrittura e modifica degli oggetti nel sistema StorageGRID.

Fasi

1. Accedere a Grid Manager utilizzando un browser supportato.
2. Nella dashboard, individuare la sezione Protocol Operations (operazioni protocollo).

   In questa sezione viene riepilogato il numero di operazioni client eseguite dal sistema StorageGRID. Le velocità dei protocolli vengono calcolate in media negli ultimi due minuti.

3. Selezionare **nodi**.
4. Dalla home page dei nodi (livello di implementazione), fare clic sulla scheda **Load Balancer**.

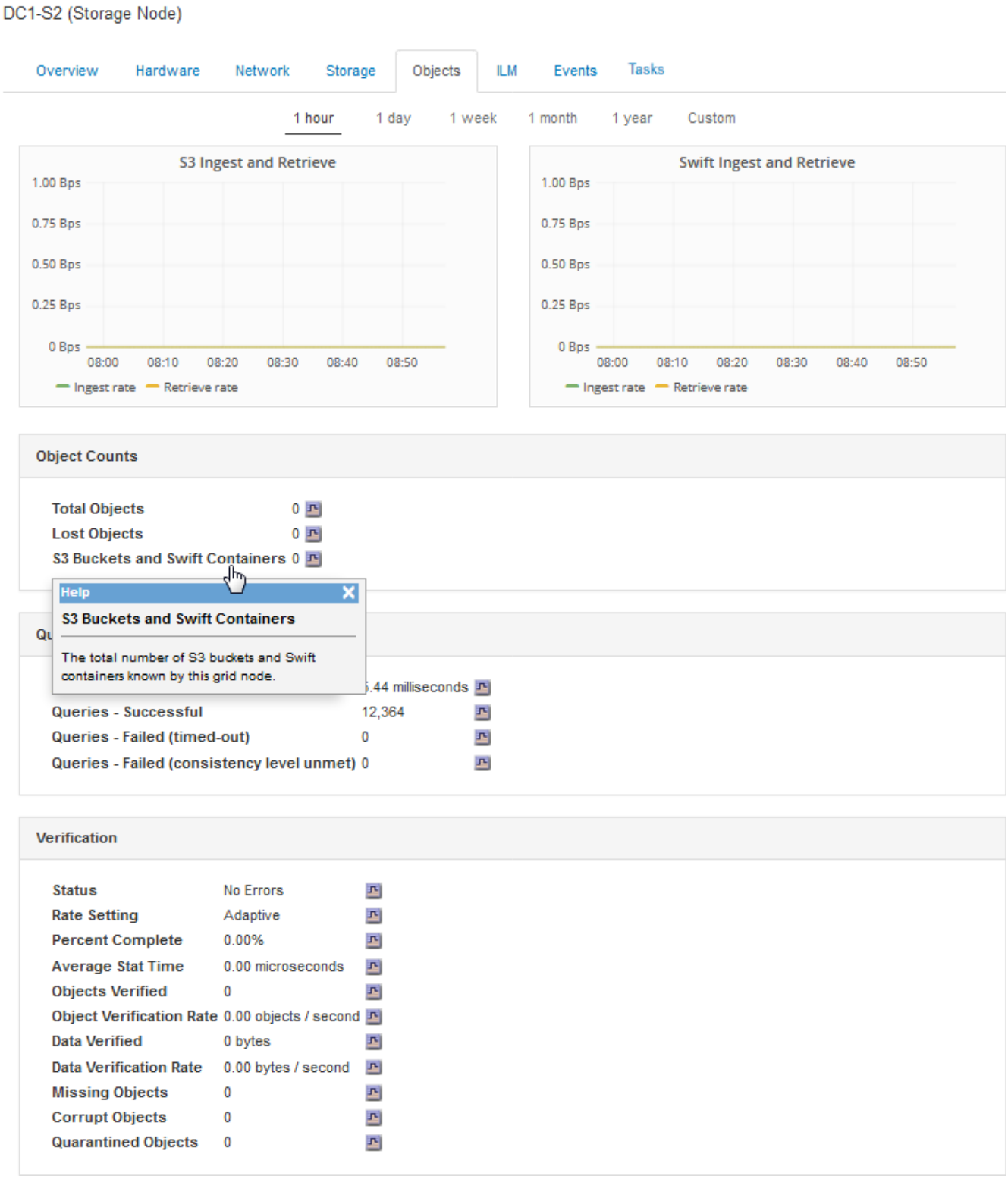
   I grafici mostrano i trend di tutto il traffico client diretto agli endpoint del bilanciamento del carico all'interno della griglia. È possibile selezionare un intervallo di tempo in ore, giorni, settimane, mesi o anni, in alternativa, è possibile applicare un intervallo personalizzato.

5. Dalla home page dei nodi (livello di implementazione), fare clic sulla scheda **oggetti**.

   Il grafico mostra le velocità di acquisizione e recupero dell'intero sistema StorageGRID in byte al secondo e byte totali. È possibile selezionare un intervallo di tempo in ore, giorni, settimane, mesi o anni, in alternativa, è possibile applicare un intervallo personalizzato.

6. Per visualizzare le informazioni relative a un nodo di storage specifico, selezionarlo dall'elenco a sinistra e fare clic sulla scheda **oggetti**.

   Il grafico mostra le velocità di acquisizione e recupero degli oggetti per questo nodo di storage. La scheda include anche metriche per il conteggio degli oggetti, le query e la verifica. È possibile fare clic sulle etichette per visualizzare le definizioni di queste metriche.



7. Se desideri ulteriori dettagli:
   a. Selezionare **supporto** > **Strumenti** > **topologia griglia**.
   b. Selezionare ***Site*** > **Overview** > **Main**.

      La sezione API Operations (operazioni API) visualizza informazioni riepilogative per l'intera griglia.

   c. Selezionare ***Storage Node*** > **LDR** > ***client application*** > **Overview** > **Main**

La sezione Operations (operazioni) visualizza informazioni riepilogative per il nodo di storage selezionato.

Accesso e revisione dei registri di audit

I messaggi di audit vengono generati dai servizi StorageGRID e memorizzati in file di log di testo. I messaggi di audit specifici delle API nei registri di audit forniscono dati critici di sicurezza, funzionamento e monitoraggio delle performance che possono aiutare a valutare lo stato di salute del sistema.

Di cosa hai bisogno

- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario disporre di `Passwords.txt` file.
- È necessario conoscere l'indirizzo IP di un nodo amministratore.

A proposito di questa attività

Il file di log di audit attivo viene denominato `audit.log`E viene memorizzato nei nodi di amministrazione.

Una volta al giorno, il file audit.log attivo viene salvato e viene avviato un nuovo file audit.log. Il nome del file salvato indica quando è stato salvato, nel formato `yyyy-mm-dd.txt`.

Dopo un giorno, il file salvato viene compresso e rinominato, nel formato `yyyy-mm-dd.txt.gz`, che conserva la data originale.

Questo esempio mostra il file audit.log attivo, il file del giorno precedente (2018-04-15.txt) e il file compresso del giorno precedente (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Fasi

1. Accedere a un nodo amministratore:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
2. Accedere alla directory contenente i file di log di controllo:`cd /var/local/audit/export`
3. Visualizzare il file di log di audit corrente o salvato, secondo necessità.

Informazioni correlate

"Esaminare i registri di audit"

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. Gli errori non vengono registrati, né le richieste di informazioni, auth o OPZIONI.

Per informazioni dettagliate sulle informazioni tracciate per le seguenti operazioni di Swift, consulta la sezione

informazioni sui messaggi di audit.

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

"Esaminare i registri di audit"

"Operazioni dell'account"

"Operazioni container"

"Operazioni a oggetti"

Informazioni sul copyright

Copyright © 2025 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 COMMERCIABILITÀ 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 CONSEQUENZIALE (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.