



Guide alle funzionalità del prodotto

StorageGRID solutions and resources

NetApp
December 12, 2025

This PDF was generated from <https://docs.netapp.com/it-it/storagegrid-enable/product-feature-guides/achieve-zero-rpo.html> on December 12, 2025. Always check docs.netapp.com for the latest.

Sommario

Guide alle funzionalità del prodotto	1
Raggiungimento di un RPO pari a zero con StorageGRID: Una guida completa alla replica multisito	1
Panoramica di StorageGRID	1
Requisiti per Zero RPO con StorageGRID	6
Implementazioni sincrone in siti multipli	6
Distribuzione multisito Single Grid	7
Distribuzione multi-sito multi-grid	11
Conclusione	13
Creazione di un pool di storage cloud per AWS o Google Cloud	14
Creazione di un pool di storage cloud per lo storage Azure Blob	15
Utilizza un pool di storage cloud per il backup	15
Configurare il servizio di integrazione della ricerca StorageGRID	16
Introduzione	16
Creare tenant e abilitare i servizi della piattaforma	17
Cerca servizi di integrazione con Amazon OpenSearch	17
Configurazione degli endpoint dei servizi della piattaforma	21
Cerca servizi di integrazione con Elasticsearch on premise	23
Configurazione degli endpoint dei servizi della piattaforma	26
Configurazione del servizio di integrazione della ricerca nel bucket	28
Dove trovare ulteriori informazioni	32
Clone del nodo	32
Considerazioni sui cloni dei nodi	32
Stime delle performance dei cloni dei nodi	33
Procedura di trasferimento del sito a griglia e di modifica della rete a livello di sito	35
Considerazioni prima del trasferimento del sito	36
Migrazione dello storage a oggetti da ONTAP S3 a StorageGRID	40
Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID	40
Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID	40
Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID	52
Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID	64
Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID	73

Guide alle funzionalità del prodotto

Raggiungimento di un RPO pari a zero con StorageGRID: Una guida completa alla replica multisito

Questo rapporto tecnico fornisce una guida completa all'implementazione di strategie di replica StorageGRID per raggiungere un Recovery Point Objective (RPO) pari a zero in caso di guasto del sito. Il documento descrive in dettaglio varie opzioni di distribuzione per StorageGRID, tra cui la replica sincrona multi-sito e la replica asincrona multi-griglia. Spiega come configurare le policy StorageGRID Information Lifecycle Management (ILM) per garantire la durabilità e la disponibilità dei dati in più sedi. Inoltre, il rapporto affronta considerazioni sulle prestazioni, scenari di errore e processi di ripristino per garantire la continuità delle operazioni dei clienti. L'obiettivo di questo documento è fornire informazioni per garantire che i dati rimangano accessibili e coerenti, anche in caso di un guasto completo del sito, sfruttando tecniche di replica sia sincrona che asincrona.

Panoramica di StorageGRID

NetApp StorageGRID è un sistema storage basato su oggetti che supporta l'API Amazon Simple Storage Service (Amazon S3) standard di settore.

StorageGRID offre un namespace singolo in siti multipli con livelli di servizio variabili determinati da policy di Information Lifecycle Management (ILM). Grazie a queste policy sul ciclo di vita puoi ottimizzare la collocazione dei tuoi dati durante tutto il loro ciclo di vita.

StorageGRID garantisce durata e disponibilità configurabili dei tuoi dati in soluzioni locali e geodistribuite. Che i tuoi dati siano in locale o in un cloud pubblico, i flussi di lavoro cloud ibridi integrati consentono alla tua azienda di sfruttare servizi cloud come Amazon Simple Notification Service (Amazon SNS), Google Cloud, Microsoft Azure Blob, Amazon S3 Glacier, Elasticsearch e molti altri.

Scala StorageGRID

Una distribuzione StorageGRID minima è composta da un nodo di amministrazione e 3 nodi di archiviazione in un unico sito. Una singola griglia può crescere fino a 220 nodi. StorageGRID può essere distribuito come un singolo sito o esteso a 16 siti.

Il nodo Admin contiene l'interfaccia di gestione, un punto centrale per le metriche e la registrazione e gestisce la configurazione dei componenti StorageGRID. Il nodo Admin contiene anche un bilanciatore del carico integrato per l'accesso all'API S3.

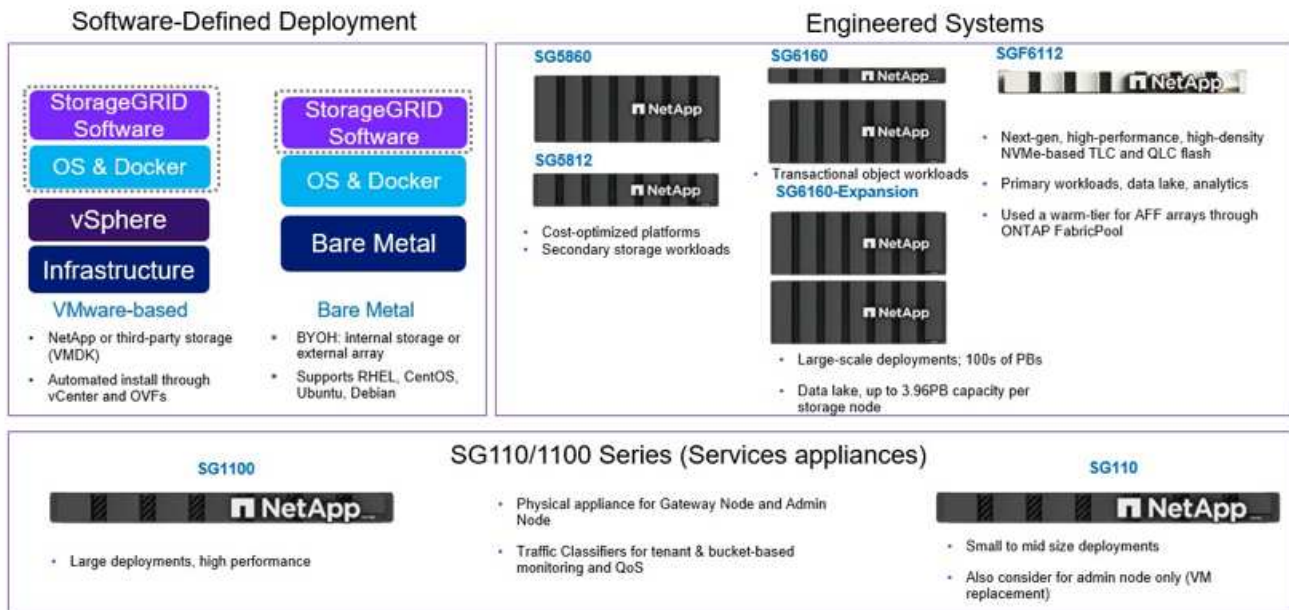
StorageGRID può essere distribuito solo come software, come appliance per macchine virtuali VMware o come appliance appositamente progettate.

Un nodo di archiviazione può essere distribuito come:

- Un nodo solo metadati che massimizza il conteggio degli oggetti
- Un nodo di archiviazione di soli oggetti che massimizza lo spazio degli oggetti
- Un nodo combinato di metadati e archiviazione di oggetti che aggiunge sia il conteggio degli oggetti che lo spazio degli oggetti

Ogni nodo di archiviazione può raggiungere una capacità di archiviazione di oggetti di diversi petabyte, consentendo un singolo namespace di centinaia di petabyte. StorageGRID fornisce anche un bilanciatore del carico integrato per le operazioni API S3 denominato nodo gateway.

Delivery paths for any workload



StorageGRID è costituito da una raccolta di nodi posizionati in una topologia di sito. Un sito in StorageGRID può essere una posizione fisica unica oppure risiedere in una posizione fisica condivisa come altri siti nella griglia come costruito logico. Un sito StorageGRID non dovrebbe estendersi su più sedi fisiche. Un sito rappresenta un'infrastruttura di rete locale (LAN) condivisa e un dominio di errore.

StorageGRID e domini di errore

StorageGRID contiene diversi livelli di domini di errore da prendere in considerazione per decidere come progettare la soluzione, come archiviare i dati e dove archiviare i dati per mitigare i rischi di guasti.

- Livello griglia - Una griglia costituita da più siti può presentare guasti o isolamento del sito e i siti accessibili possono continuare a funzionare come rete.
- Livello sito - i guasti all'interno di un sito possono influire sulle operazioni del sito, ma non sul resto della griglia.
- Livello nodo - il guasto di Un nodo non influisce sul funzionamento del sito.
- Livello disco - un guasto del disco non influisce sul funzionamento del nodo.

Dati e metadati di oggetti

Con lo storage a oggetti, l'unità di storage è un oggetto, piuttosto che un file o un blocco. A differenza della gerarchia ad albero di un file system o di uno storage a blocchi, lo storage a oggetti organizza i dati in un layout piatto e non strutturato. Lo storage a oggetti separa la posizione fisica dei dati dal metodo utilizzato per memorizzare e recuperare tali dati.

Ogni oggetto in un sistema di storage basato su oggetti ha due parti: Dati oggetto e metadati oggetto.

- I dati oggetto rappresentano i dati sottostanti effettivi, ad esempio una fotografia, un filmato o una cartella clinica.
- I metadati degli oggetti sono informazioni che descrivono un oggetto.

StorageGRID utilizza i metadati degli oggetti per tenere traccia delle posizioni di tutti gli oggetti nella griglia e gestire il ciclo di vita di ciascun oggetto nel tempo.

I metadati dell'oggetto includono informazioni come:

- Metadati di sistema, tra cui un ID univoco per ciascun oggetto, il nome dell'oggetto, il nome del bucket S3, il nome o l'ID dell'account tenant, la dimensione logica dell'oggetto, la data e l'ora in cui l'oggetto è stato creato per la prima volta e la data e l'ora dell'ultima modifica dell'oggetto.
- Posizione di archiviazione corrente della copia replicata o del frammento con codice di cancellazione di ciascun oggetto.
- Qualsiasi coppia di valori chiave metadati utente personalizzata associata all'oggetto.
- Per gli oggetti S3, qualsiasi coppia chiave-valore tag oggetto associata all'oggetto
- Per oggetti segmentati e oggetti multiparte, identificatori di segmento e dimensioni dei dati.

I metadati degli oggetti sono personalizzabili ed espandibili, il che lo rende flessibile per l'utilizzo da parte delle applicazioni. Per informazioni dettagliate su come e dove StorageGRID archivia i metadati degli oggetti, visitare il sito ["Gestire lo storage dei metadati degli oggetti"](#).

Il sistema Information Lifecycle management (ILM) di StorageGRID viene utilizzato per orchestrare il posizionamento, la durata e il comportamento di acquisizione per tutti i dati degli oggetti nel sistema StorageGRID. Le regole ILM determinano il modo in cui StorageGRID archivia gli oggetti nel tempo utilizzando repliche degli oggetti o erasure coding dell'oggetto nei nodi e nei siti. Questo sistema ILM è responsabile della coerenza dei dati degli oggetti all'interno di una griglia.

Erasure coding

StorageGRID offre la possibilità di cancellare i dati del codice a livello di nodo e a livello di unità. Con gli apparecchi StorageGRID cancelliamo tramite codice i dati memorizzati su ciascun nodo su tutte le unità presenti nel nodo, garantendo protezione locale contro guasti di più dischi che causano perdite o interruzioni di dati. Le ricostruzioni in seguito a guasti delle unità sono locali al nodo e non richiedono la replica dei dati sulla rete.

Inoltre, gli apparecchi StorageGRID utilizzano schemi di codifica di cancellazione per archiviare i dati degli oggetti nei nodi all'interno di un sito o distribuiti su 3 o più siti nel sistema StorageGRID tramite le regole ILM di StorageGRID che proteggono dai guasti dei nodi.

La codifica di cancellazione fornisce un layout di archiviazione resiliente ai guasti dei nodi e dei siti con un overhead inferiore rispetto alla replica. Tutti gli schemi di codifica di cancellazione StorageGRID possono essere implementati in un singolo sito, a condizione che venga raggiunto il numero minimo di nodi necessari per archiviare i blocchi di dati. Ciò significa che per uno schema EC 4+2 devono essere disponibili almeno 6 nodi per ricevere i dati.

Erasure-coding scheme ($k+m$)	Minimum number of deployed sites	Recommended number of Storage Nodes at each site	Total recommended number of Storage Nodes	Site loss protection?	Storage overhead
4+2	3	3	9	Yes	50%
6+2	4	3	12	Yes	33%
8+2	5	3	15	Yes	25%
6+3	3	4	12	Yes	50%
9+3	4	4	16	Yes	33%
2+1	3	3	9	Yes	50%
4+1	5	3	15	Yes	25%
6+1	7	3	21	Yes	17%
7+5	3	5	15	Yes	71%

Coerenza dei metadati

In StorageGRID, i metadati vengono generalmente archiviati con tre repliche per sito, per garantire coerenza e disponibilità. Questa ridondanza contribuisce a mantenere l'integrità e l'accessibilità dei dati anche in caso di errore.

La coerenza predefinita è definita a livello di griglia. Gli utenti possono modificare la coerenza a livello del bucket in qualsiasi momento.

Le opzioni di coerenza delle benne disponibili in StorageGRID sono:

- **Tutti:** Offre il massimo livello di coerenza. Tutti i nodi nella griglia ricevono i dati immediatamente, altrimenti la richiesta non riesce.
- **Forte-globale:**
 - **Legacy Strong Global:** garantisce la coerenza di lettura e scrittura per tutte le richieste dei clienti su tutti i siti.
 - Questo è il comportamento predefinito per tutti i sistemi aggiornati dalla versione 11.9 o precedente alla versione 12.0 senza passare manualmente al nuovo Quorum Strong Global.
 - **Quorum Strong-global:** garantisce la coerenza di lettura e scrittura per tutte le richieste dei clienti su tutti i siti. Offre coerenza per più nodi o persino in caso di errore del sito se è possibile raggiungere il quorum di replica dei metadati.
 - Questo è il comportamento predefinito per tutti i sistemi appena installati alla versione 12.0 o successiva.
 - La coerenza del QUORUM è definita come un quorum di repliche di metadati del nodo di archiviazione, in cui ogni sito ha 3 repliche di metadati. Può essere calcolato come segue: $1 + ((N * 3) / 2)$ dove N è il numero totale di siti
 - Ad esempio, è necessario effettuare almeno 5 repliche da una griglia a 3 siti, con un massimo di 3

repliche all'interno di un sito.

- **Strong-Site:** Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
- **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.
- **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.

Coerenza dei dati degli oggetti

Mentre i metadati vengono replicati automaticamente all'interno e tra i siti, spetta a te prendere decisioni sul posizionamento dello storage dei dati a oggetti. I dati degli oggetti possono essere memorizzati in repliche all'interno e tra i siti, con erasure coding all'interno o tra i siti, o in una combinazione o repliche e schemi di storage con erasure coding. Le regole ILM possono essere applicate a tutti gli oggetti o filtrate per applicarsi solo a determinati oggetti, bucket o tenant. Le regole ILM definiscono il modo in cui gli oggetti vengono memorizzati, le repliche e/o il erasure coding, la durata della memorizzazione degli oggetti in tali posizioni, se il numero di repliche o lo schema di erasure coding deve cambiare o se le posizioni devono cambiare nel tempo.

Ogni regola ILM verrà configurata con uno dei tre comportamenti di acquisizione per la protezione degli oggetti: Dual commit, balanced o Strict.

L'opzione di doppio commit eseguirà immediatamente due copie su due nodi di archiviazione diversi nella griglia e restituirà al client la richiesta di esito positivo. La selezione del nodo verrà tentata all'interno del sito della richiesta, ma in alcune circostanze potrebbe utilizzare nodi di un altro sito. L'oggetto viene aggiunto alla coda ILM per essere valutato e posizionato in base alle regole ILM.

L'opzione bilanciata valuta immediatamente l'oggetto in base alla policy ILM e lo posiziona in modo sincrono prima di restituire la richiesta di esito positivo al client. Se la regola ILM non può essere rispettata immediatamente a causa di un'interruzione o di uno spazio di archiviazione inadeguato per soddisfare i requisiti di posizionamento, verrà utilizzato il doppio commit. Una volta risolto il problema, ILM posizionerà automaticamente l'oggetto in base alla regola definita.

L'opzione strict valuta immediatamente l'oggetto in base alla policy ILM e lo posiziona in modo sincrono prima di restituire la richiesta di esito positivo al client. Se la regola ILM non può essere soddisfatta immediatamente a causa di un'interruzione o di uno spazio di archiviazione inadeguato per soddisfare i requisiti di posizionamento, la richiesta non andrà a buon fine e il client dovrà riprovare.

Bilanciamento del carico

StorageGRID può essere implementato con accesso client tramite i nodi gateway integrati, un bilanciatore di carico esterno di 3^e parti, round robin DNS o direttamente in un nodo storage. È possibile implementare diversi nodi di gateway in un sito e configurarli in gruppi a disponibilità elevata per offrire failover e failback automatici in caso di black-out di un nodo di gateway. È possibile combinare metodi di bilanciamento del carico in una soluzione per fornire un unico punto di accesso per tutti i siti in una soluzione.

Per impostazione predefinita, i nodi gateway bilanciano il carico tra i nodi di archiviazione nel sito in cui risiede il nodo gateway. StorageGRID può essere configurato per consentire ai nodi gateway di bilanciare il carico utilizzando nodi provenienti da più siti. Questa configurazione aggiungerebbe la latenza tra quei siti alla latenza di risposta alle richieste del client. Questa impostazione dovrebbe essere configurata solo se la latenza totale è accettabile per i client.

È possibile garantire un RTO pari a zero combinando il bilanciamento del carico locale e globale. Per garantire un accesso client ininterrotto è necessario bilanciare il carico delle richieste client. Una soluzione StorageGRID può contenere molti nodi gateway e gruppi ad alta disponibilità in ogni sito. Per garantire un accesso ininterrotto ai client in qualsiasi sito, anche in caso di guasto del sito, è necessario configurare una soluzione di bilanciamento del carico esterno in combinazione con i nodi StorageGRID Gateway. Configurare gruppi ad alta disponibilità del nodo Gateway che gestiscono il carico all'interno di ciascun sito e utilizzare il bilanciatore del carico esterno per bilanciare il carico tra i gruppi ad alta disponibilità. Il bilanciatore del carico esterno deve essere configurato per eseguire un controllo dello stato di integrità per garantire che le richieste vengano inviate solo ai siti operativi. Per ulteriori informazioni sul bilanciamento del carico con StorageGRID, consultare ["Report tecnico per il bilanciamento del carico di StorageGRID"](#).

Requisiti per Zero RPO con StorageGRID

Per raggiungere l'obiettivo RPO (Recovery Point Objective) zero in un sistema storage a oggetti, è fondamentale che al momento del guasto:

- Sia i metadati che i contenuti degli oggetti sono sincronizzati e considerati coerenti
- I contenuti degli oggetti rimangono accessibili nonostante il guasto.

Per una distribuzione multi-sito, Quorum Strong Global è il modello di coerenza preferito per garantire che i metadati siano sincronizzati su tutti i siti, rendendolo essenziale per soddisfare il requisito RPO zero.

Gli oggetti nel sistema di archiviazione vengono archiviati in base alle regole di Information Lifecycle Management (ILM), che stabiliscono come e dove i dati vengono archiviati durante il loro ciclo di vita. Per la replica sincrona, è possibile prendere in considerazione l'esecuzione rigorosa o l'esecuzione bilanciata.

- Per un RPO pari a zero è necessaria un'esecuzione rigorosa di queste regole ILM, in quanto assicura che gli oggetti vengano posizionati nelle posizioni definite senza alcun ritardo o fallback, mantenendo la disponibilità e la coerenza dei dati.
- Il comportamento di acquisizione ILM di StorageGRID offre un equilibrio tra alta disponibilità e resilienza, consentendo agli utenti di continuare ad acquisire i dati anche in caso di guasto del sito.

Implementazioni sincrone in siti multipli

Soluzioni multi-sito: StorageGRID consente di replicare oggetti su più siti all'interno della griglia in modo sincrono. Impostando regole di Information Lifecycle Management (ILM) con comportamento bilanciato o rigoroso, gli oggetti vengono posizionati immediatamente nelle posizioni specificate. Anche la configurazione del livello di coerenza del bucket su Quorum Strong Global garantirà la replica sincrona dei metadati. StorageGRID utilizza un singolo namespace globale, memorizzando le posizioni di posizionamento degli oggetti come metadati, in modo che ogni nodo sappia dove si trovano tutte le copie o i pezzi codificati per la cancellazione. Se un oggetto non può essere recuperato dal sito in cui è stata effettuata la richiesta, verrà recuperato automaticamente da un sito remoto senza bisogno di procedure di failover.

Una volta risolto il problema, non è necessario alcun intervento di fallback manuale. Le performance di replica dipendono dal sito con il throughput di rete più basso, la latenza più alta e le performance più basse. Le prestazioni di un sito si basano sul numero di nodi, sul numero di core della CPU e sulla velocità, sulla memoria, sulla quantità di unità e sui tipi di unità.

Soluzioni multi-grid: StorageGRID è in grado di replicare tenant, utenti e bucket tra più sistemi StorageGRID utilizzando la replica cross-grid (CGR, Cross-Grid Replication). CGR può estendere i dati selezionati a più di 16 siti, aumentare la capacità utilizzabile dell'archivio di oggetti e fornire il disaster recovery. La replica dei bucket con CGR include oggetti, versioni degli oggetti e metadati e può essere bidirezionale o unidirezionale. L'RPO (Recovery Point Objective) dipende dalle prestazioni di ogni sistema StorageGRID e dalle connessioni

di rete tra di essi.

Sommario:

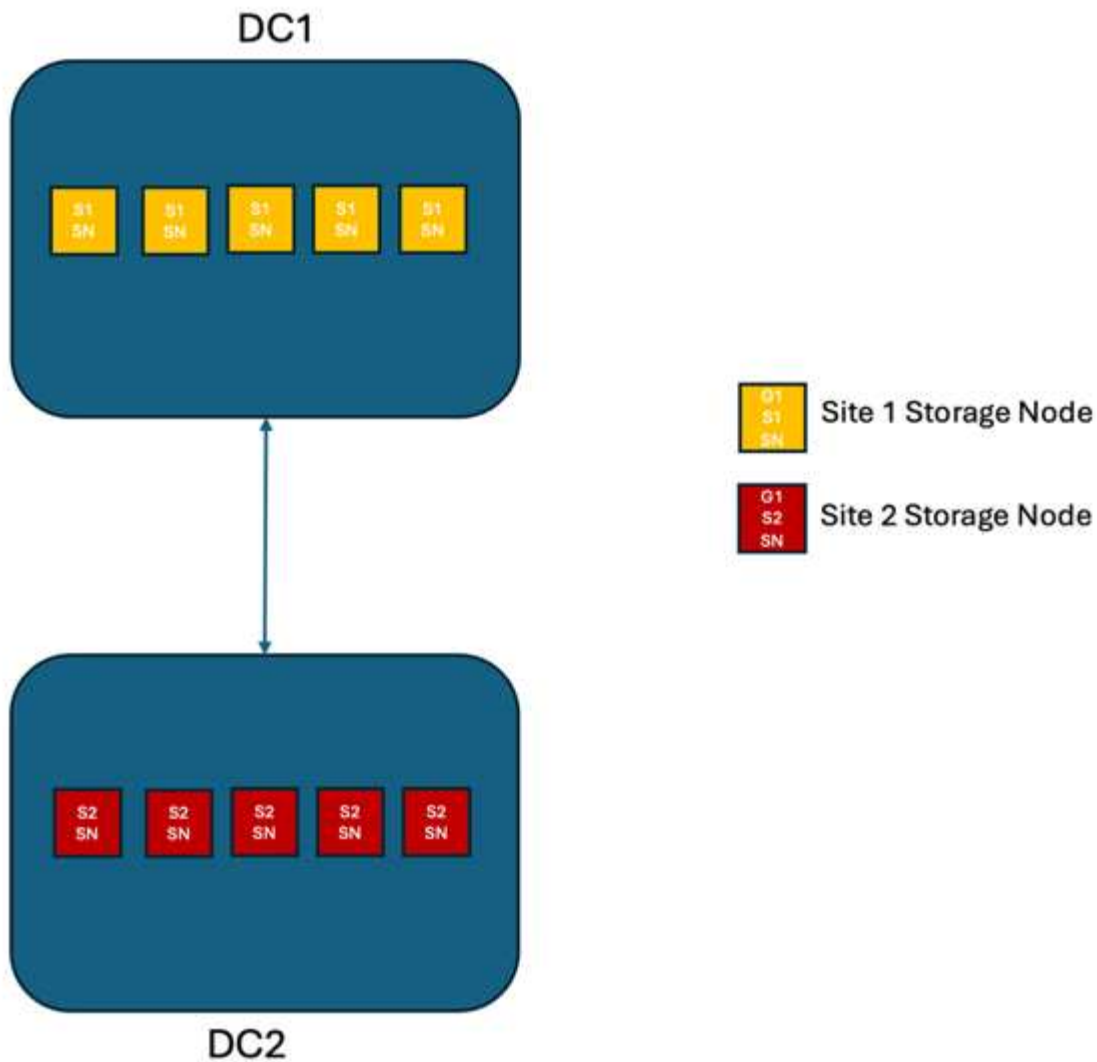
- La replica intra-grid include una replica sincrona e asincrona, configurabile tramite comportamento di acquisizione ILM e controllo della coerenza dei metadati.
- La replica inter-grid è solo asincrona.

Distribuzione multisito Single Grid

Negli scenari seguenti, le soluzioni StorageGRID sono configurate con un bilanciatore del carico esterno opzionale che gestisce le richieste ai gruppi ad alta disponibilità del bilanciatore del carico integrato. In questo modo si otterrà un RTO pari a zero, oltre a un RPO pari a zero. ILM è configurato con protezione di ingestione bilanciata per il posizionamento sincrono. Ogni bucket è configurato con la versione Quorum del modello di coerenza Strong Global per griglie di 3 o più siti e con la versione Legacy del modello di coerenza Strong Global per 2 siti.

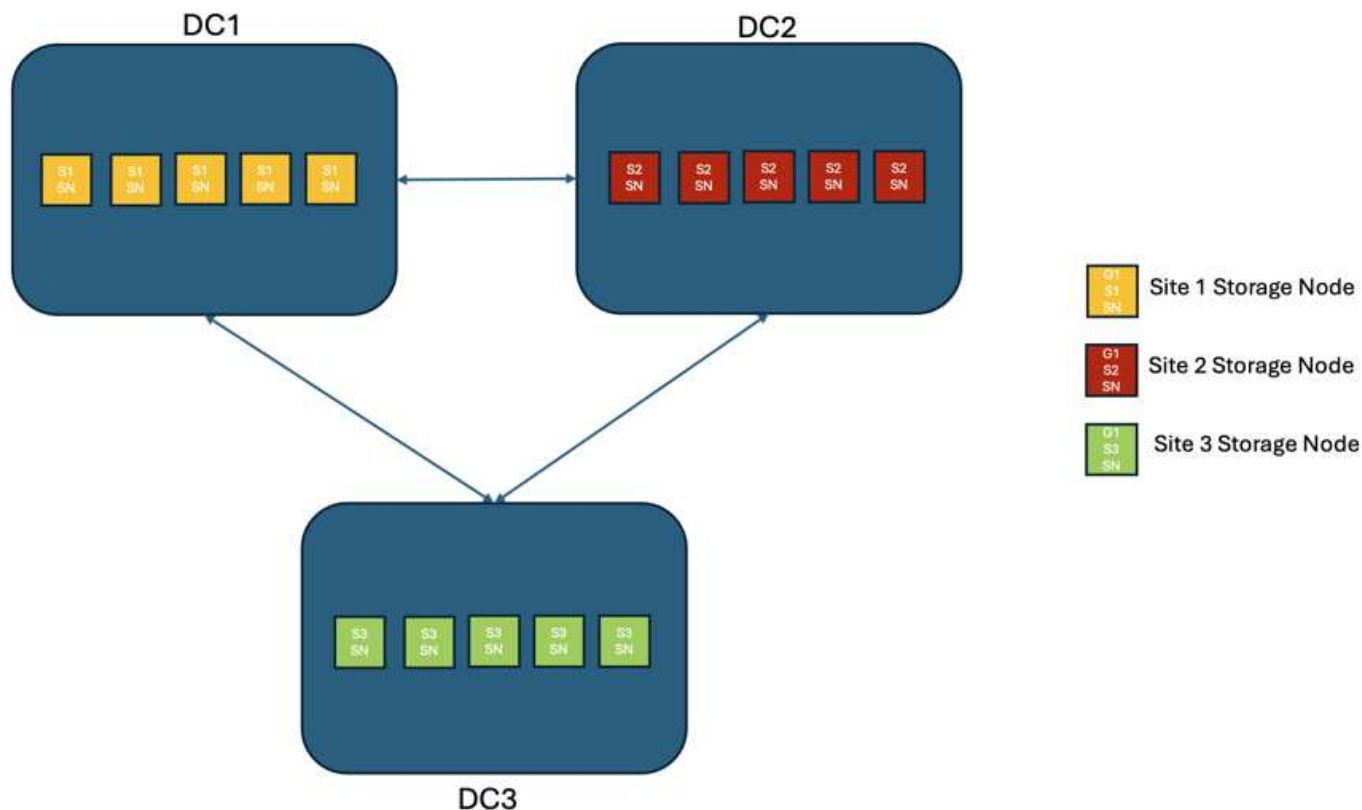
Scenario 1:

In una soluzione StorageGRID a due siti, sono presenti almeno due repliche di ogni oggetto e 6 repliche di tutti i metadati. In caso di ripristino dopo un errore, gli aggiornamenti dall'interruzione verranno sincronizzati automaticamente con il sito/nodi ripristinati. Con solo 2 siti, è improbabile che si riesca a raggiungere un RPO pari a zero in scenari di guasto che vanno oltre la perdita completa del sito.



Scenario 2:

In una soluzione StorageGRID di tre o più siti, sono presenti almeno 3 repliche o 3 blocchi EC di ogni oggetto e 9 repliche di tutti i metadati. In caso di ripristino dopo un errore, gli aggiornamenti dall'interruzione verranno sincronizzati automaticamente con il sito/nodi ripristinati. Con tre o più siti è possibile raggiungere un RPO pari a zero.



Scenari di guasti su più siti

Guasto	Risultato a 2 siti + Legacy Strong Global	3 o più siti risultato + Quorum Strong Global
Guasto al disco a nodo singolo	Ogni appliance utilizza gruppi di dischi multipli e può sostenere almeno 1 dischi per gruppo di guasti senza interruzioni o perdita di dati.	Ogni appliance utilizza gruppi di dischi multipli e può sostenere almeno 1 dischi per gruppo di guasti senza interruzioni o perdita di dati.
Guasto a un singolo nodo in un sito	Nessuna interruzione delle operazioni o perdita di dati.	Nessuna interruzione delle operazioni o perdita di dati.
Guasto a più nodi in un solo sito	Interruzione delle operazioni dei client dirette a questo sito senza perdita di dati. Le operazioni dirette all'altro sito rimangono senza interruzioni e non perdono dati.	Le operazioni vengono dirette a tutti gli altri siti mantenendo interruzioni e senza perdita di dati.

Guasto	Risultato a 2 siti + Legacy Strong Global	3 o più siti risultato + Quorum Strong Global
Guasto a nodo singolo in più siti	<p>Nessuna interruzione o perdita di dati se:</p> <ul style="list-style-type: none"> • Esiste almeno una copia replicata nella griglia • Nella griglia sono presenti frammenti EC sufficienti <p>Operazioni interrotte e rischio di perdita di dati se:</p> <ul style="list-style-type: none"> • Non esistono copie replicate • Presenza di mandrini EC insufficienti 	<p>Nessuna interruzione o perdita di dati se:</p> <ul style="list-style-type: none"> • Esiste almeno una singola copia replicata nella griglia • Nella griglia sono presenti frammenti EC sufficienti <p>Operazioni interrotte e rischio di perdita di dati se:</p> <ul style="list-style-type: none"> • Non esistono copie replicate • Non esistono chunks EC sufficienti per recuperare l'oggetto
Guasto a un singolo sito	<p>Alcune operazioni del client verranno interrotte finché il problema non verrà risolto. Le operazioni GET e HEAD continueranno senza interruzioni. Ridurre la coerenza del bucket a lettura dopo nuova scrittura o inferiore per continuare le operazioni senza interruzioni in questo stato di errore.</p>	<p>Nessuna interruzione delle operazioni o perdita di dati.</p>
Guasti a un singolo sito e a un nodo singolo	<p>Alcune operazioni del client verranno interrotte finché il problema non verrà risolto. Le operazioni HEAD continueranno senza interruzioni. Le operazioni GET continueranno senza interruzioni se esiste una copia replicata o un numero sufficiente di blocchi EC. Ridurre la coerenza del bucket a lettura dopo nuova scrittura o inferiore per continuare le operazioni senza interruzioni in questo stato di errore.</p>	<p>Nessuna interruzione delle operazioni o perdita di dati. Possibile perdita di dati a seconda del numero di copie replicate. La codifica Local Erasure può impedire la perdita di dati.</p>

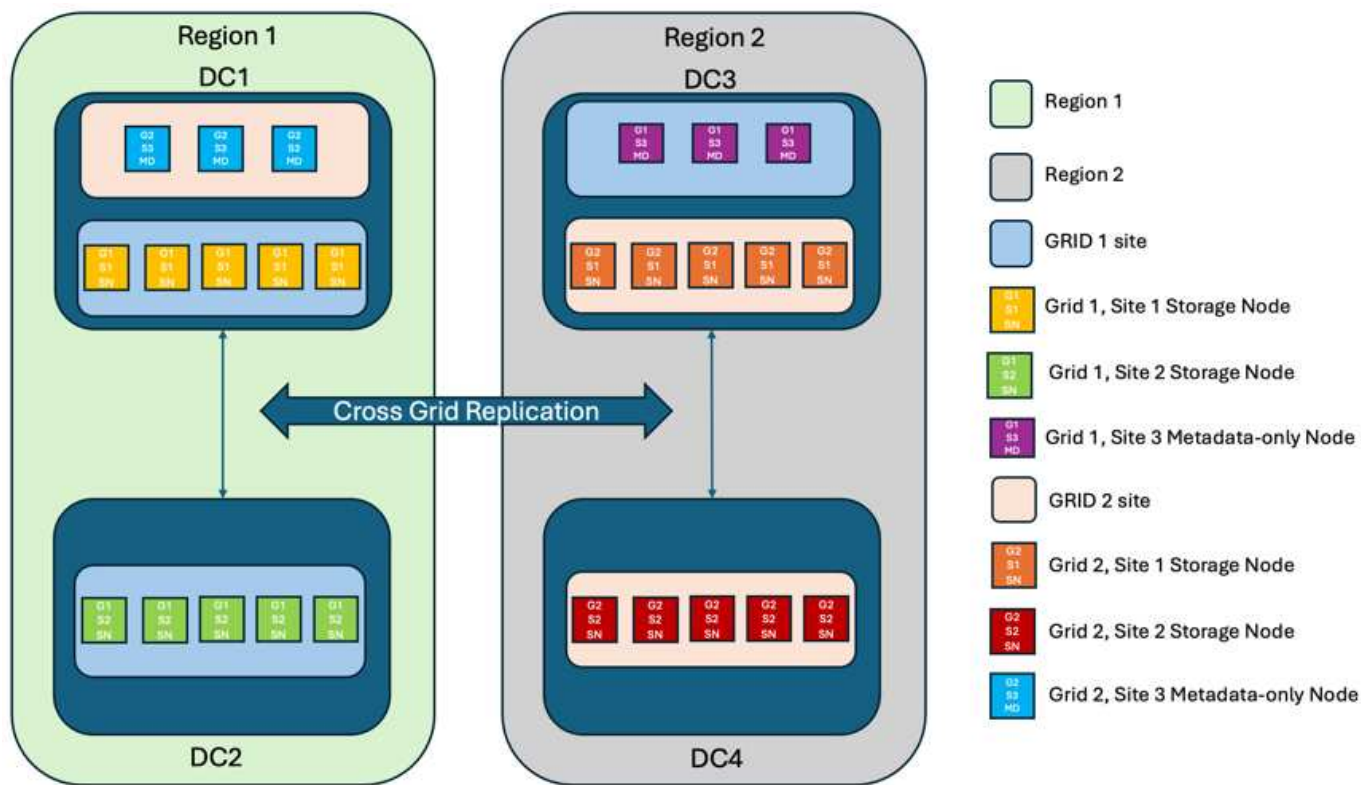
Guasto	Risultato a 2 siti + Legacy Strong Global	3 o più siti risultato + Quorum Strong Global
Singolo sito più un nodo da ciascun sito rimanente	Esistono solo due siti. Vedere: Singolo sito più un singolo nodo.	Le operazioni verranno interrotte se non sarà possibile raggiungere il quorum della replica dei metadati. Ridurre la coerenza del bucket a lettura dopo nuova scrittura o inferiore per continuare le operazioni senza interruzioni in questo stato di errore. Possibile perdita di dati per guasto permanente a seconda del numero di copie replicate. La codifica Local Erasure può impedire la perdita di dati.
Guasto multi-sito	Non rimangono siti operativi. I dati andranno persi se almeno un sito non potrà essere recuperato nella sua interezza.	Le operazioni verranno interrotte se non sarà possibile raggiungere il quorum della replica dei metadati. Ridurre la coerenza del bucket a lettura dopo nuova scrittura o inferiore per continuare le operazioni senza interruzioni in questo stato di errore. Possibile perdita di dati per guasto permanente se non rimangono sufficienti blocchi codificati per la cancellazione. La codifica di cancellazione locale o le copie replicate possono impedire la perdita di dati.
Isolamento della rete di un sito	le operazioni del client saranno interrotte finché il problema non sarà risolto. Ridurre la coerenza del bucket a lettura dopo nuova scrittura o inferiore per continuare le operazioni senza interruzioni in questo stato di errore. Nessuna perdita di dati	Le operazioni saranno interrotte per il sito isolato, ma non si verificherà alcuna perdita di dati. Ridurre la coerenza del bucket a lettura dopo nuova scrittura o inferiore per continuare le operazioni senza interruzioni in questo stato di errore. Nessuna interruzione delle operazioni nei siti rimanenti e nessuna perdita di dati.

Distribuzione multi-sito multi-grid

Per aggiungere un ulteriore livello di ridondanza, questo scenario impiegherà due cluster StorageGRID e utilizzerà la replica tra griglie per mantenerli sincronizzati. Per questa soluzione, ogni cluster StorageGRID avrà tre siti. Due siti saranno utilizzati per l'archiviazione degli oggetti e dei metadati, mentre il terzo sito sarà utilizzato esclusivamente per i metadati. Entrambi i sistemi saranno configurati con una regola ILM bilanciata per archiviare in modo sincrono gli oggetti utilizzando la codifica di cancellazione in ciascuno dei due siti dati. I bucket saranno configurati con il modello di coerenza globale Quorum Strong. Ogni griglia sarà configurata con replica bidirezionale tra griglie su ogni bucket. Ciò garantisce la replicazione asincrona tra le regioni. Facoltativamente, è possibile implementare un bilanciatore del carico globale per gestire le richieste ai gruppi ad alta disponibilità del bilanciatore del carico integrato di entrambi i sistemi StorageGRID per ottenere un

RPO pari a zero.

La soluzione utilizzerà quattro posizioni equamente suddivise in due regioni. La regione 1 conterrà i 2 siti di memorizzazione della griglia 1 come griglia primaria della regione e il sito di metadati della griglia 2. La regione 2 conterrà i 2 siti di memorizzazione della griglia 2 come griglia primaria della regione e il sito di metadati della griglia 1. In ogni regione la stessa posizione può ospitare il sito di archiviazione della griglia primaria della regione e il sito di sola metadati della griglia delle altre regioni. L'utilizzo dei soli nodi di metadati come il terzo sito fornirà la coerenza richiesta per i metadati, non duplicando lo storage degli oggetti in tale posizione.



Questa soluzione con quattro ubicazioni separate offre ridondanza completa di due sistemi StorageGRID separati che mantengono un RPO di 0 e sfrutteranno sia la replica sincrona multi-sito che la replica asincrona multi-grid. È possibile guastare qualsiasi sito mantenendo operazioni client senza interruzioni su entrambi i sistemi StorageGRID.

Questa soluzione prevede quattro copie sottoposte a erasure coding per ciascun oggetto e 18 repliche di tutti i metadati. Ciò consente più scenari di errore senza impatto sulle operazioni dei client. In caso di errore, gli aggiornamenti del ripristino dal black-out verranno sincronizzati automaticamente con il sito/i nodi guasti.

Scenari di guasto multisito e multi-grid

Guasto	Risultato
Guasto al disco a nodo singolo	Ogni appliance utilizza gruppi di dischi multipli e può sostenere almeno 1 dischi per gruppo di guasti senza interruzioni o perdita di dati.
Guasto a un singolo nodo in un sito in un grid	Nessuna interruzione delle operazioni o perdita di dati.
Guasto a un singolo nodo in un sito in ciascun grid	Nessuna interruzione delle operazioni o perdita di dati.

Guasto	Risultato
Guasto di più nodi in un sito in una griglia	Nessuna interruzione delle operazioni o perdita di dati.
Guasto a più nodi in un sito in ciascun grid	Nessuna interruzione delle operazioni o perdita di dati.
Guasto a un singolo nodo in più siti in un grid	Nessuna interruzione delle operazioni o perdita di dati.
Guasto a un singolo nodo in più siti in ciascun grid	Nessuna interruzione delle operazioni o perdita di dati.
Guasto a un singolo sito in una griglia	Nessuna interruzione delle operazioni o perdita di dati.
Guasto a un singolo sito in ciascun grid	Nessuna interruzione delle operazioni o perdita di dati.
Guasti a un singolo sito e a un nodo in un grid	Nessuna interruzione delle operazioni o perdita di dati.
Singolo sito più un nodo da ciascun sito rimanente in un singolo grid	Nessuna interruzione delle operazioni o perdita di dati.
Errore di singola posizione	Nessuna interruzione delle operazioni o perdita di dati.
Errore di singola posizione in ciascuna griglia DC1 e DC3	Le operazioni verranno interrotte fino a quando il guasto non verrà risolto o la coerenza del bucket non verrà ridotta; ogni grid avrà perso 2 siti Tutti i dati sono ancora presenti in 2 postazioni
Errore di singola posizione in ciascuna griglia DC1 e DC4 o DC2 e DC3	Nessuna interruzione delle operazioni o perdita di dati.
Errore di singola posizione in ciascuna griglia DC2 e DC4	Nessuna interruzione delle operazioni o perdita di dati.
Isolamento della rete di un sito	Le operazioni per il sito isolato verranno interrotte, ma nessun dato andrà perso Nessuna interruzione delle operazioni nei siti rimanenti o perdita di dati.

Conclusione

L'obiettivo di zero recovery point objective (RPO) con StorageGRID è un obiettivo critico per garantire la conservazione e la disponibilità dei dati in caso di guasti del sito. Sfruttando le solide strategie di replica di StorageGRID, tra cui la replica sincrona multisito e la replica asincrona multi-grid, le organizzazioni possono mantenere operazioni ininterrotte dei client e garantire la coerenza dei dati in più posizioni. L'implementazione delle policy ILM (Information Lifecycle Management) e l'utilizzo di nodi basati solo sui metadati migliorano ulteriormente la resilienza e le prestazioni del sistema. Con StorageGRID, le aziende possono gestire con

sicurezza i propri dati, sapendo che rimangono accessibili e coerenti anche in caso di complessi scenari di guasto. Questo approccio completo alla gestione e alla replica dei dati sottolinea l'importanza di una pianificazione e di un'esecuzione meticolose per il raggiungimento di un RPO pari a zero e la salvaguardia di informazioni preziose.

Creazione di un pool di storage cloud per AWS o Google Cloud

È possibile utilizzare un pool di storage cloud se si desidera spostare gli oggetti StorageGRID in un bucket S3 esterno. Il bucket esterno può appartenere ad Amazon S3 (AWS) o Google Cloud.

Di cosa hai bisogno

- StorageGRID 11.6 è stato configurato.
- Hai già configurato un bucket S3 esterno su AWS o Google Cloud.

Fasi

1. In Grid Manager, selezionare **ILM > Storage Pools**.
2. Nella sezione Cloud Storage Pools della pagina, selezionare **Create**.

Viene visualizzata la finestra a comparsa Create Cloud Storage Pool (Crea pool di storage cloud).

3. Inserire un nome visualizzato.
4. Selezionare **Amazon S3** dall'elenco a discesa Provider Type (tipo di provider).

Questo tipo di provider funziona per AWS S3 o Google Cloud.

5. Immettere l'URI per il bucket S3 da utilizzare per il Cloud Storage Pool.

Sono consentiti due formati:

`https://host:port`

`http://host:port`

6. Immettere il nome del bucket S3.

Il nome specificato deve corrispondere esattamente al nome del bucket S3; in caso contrario, la creazione del pool di storage cloud non riesce. Non è possibile modificare questo valore dopo il salvataggio del Cloud Storage Pool.

7. Se si desidera, inserire l'ID della chiave di accesso e la chiave di accesso segreta.
8. Selezionare **non verificare certificato** dall'elenco a discesa.
9. Fare clic su **Save** (Salva).

Risultato previsto

Verificare che sia stato creato un Cloud Storage Pool per Amazon S3 o Google Cloud.

Di Jonathan Wong

Creazione di un pool di storage cloud per lo storage Azure Blob

È possibile utilizzare un pool di storage cloud se si desidera spostare gli oggetti StorageGRID in un container Azure esterno.

Di cosa hai bisogno

- StorageGRID 11.6 è stato configurato.
- Hai già configurato un container Azure esterno.

Fasi

1. In Grid Manager, selezionare **ILM > Storage Pools**.
2. Nella sezione Cloud Storage Pools della pagina, selezionare **Create**.

Viene visualizzata la finestra a comparsa Create Cloud Storage Pool (Crea pool di storage cloud).

3. Inserire un nome visualizzato.
4. Selezionare **Azure Blob Storage** dall'elenco a discesa Provider Type (tipo di provider).
5. Immettere l'URI per il bucket S3 da utilizzare per il Cloud Storage Pool.

Sono consentiti due formati:

`https://host:port`

`http://host:port`

6. Immettere il nome del container Azure.

Il nome specificato deve corrispondere esattamente al nome del container Azure; in caso contrario, la creazione del pool di storage cloud non riesce. Non è possibile modificare questo valore dopo il salvataggio del Cloud Storage Pool.

7. Facoltativamente, inserire il nome account associato al container Azure e la chiave account per l'autenticazione.
8. Selezionare **non verificare certificato** dall'elenco a discesa.
9. Fare clic su **Save** (Salva).

Risultato previsto

Verificare che sia stato creato un pool di storage cloud per Azure Blob Storage.

Di Jonathan Wong

Utilizza un pool di storage cloud per il backup

È possibile creare una regola ILM per spostare gli oggetti in un Cloud Storage Pool per il backup.

Di cosa hai bisogno

- StorageGRID 11.6 è stato configurato.
- Hai già configurato un container Azure esterno.

Fasi

1. In Grid Manager, selezionare **ILM** > **Rules** > **Create**.
2. Inserire una descrizione.
3. Inserire un criterio per attivare la regola.
4. Fare clic su **Avanti**.
5. Replicare l'oggetto nei nodi di storage.
6. Aggiungere una regola di posizionamento.
7. Replicare l'oggetto nel Cloud Storage Pool
8. Fare clic su **Avanti**.
9. Fare clic su **Save** (Salva).

Risultato previsto

Verificare che il diagramma di conservazione mostri gli oggetti memorizzati localmente in StorageGRID e in un pool di storage cloud per il backup.

Verificare che, quando viene attivata la regola ILM, esista una copia nel Cloud Storage Pool ed è possibile recuperare l'oggetto localmente senza eseguire un ripristino dell'oggetto.

Di Jonathan Wong

Configurare il servizio di integrazione della ricerca StorageGRID

Questa guida fornisce istruzioni dettagliate per la configurazione del servizio di integrazione della ricerca NetApp StorageGRID con il servizio Amazon OpenSearch o Elasticsearch on-premise.

Introduzione

StorageGRID supporta tre tipi di servizi di piattaforma.

- **Replica di StorageGRID CloudMirror.** Eseguire il mirroring di oggetti specifici da un bucket StorageGRID a una destinazione esterna specificata.
- **Notifiche.** Notifiche di eventi per bucket per inviare notifiche su azioni specifiche eseguite su oggetti a un servizio Amazon Simple Notification Service (Amazon SNS) esterno specificato.
- **Ricerca servizio di integrazione.** Inviare metadati di oggetti Simple Storage Service (S3) a un indice Elasticsearch specificato, in cui è possibile cercare o analizzare i metadati utilizzando il servizio esterno.

I servizi della piattaforma vengono configurati dal tenant S3 tramite l'interfaccia utente di Tenant Manager. Per ulteriori informazioni, vedere ["Considerazioni sull'utilizzo dei servizi della piattaforma"](#).

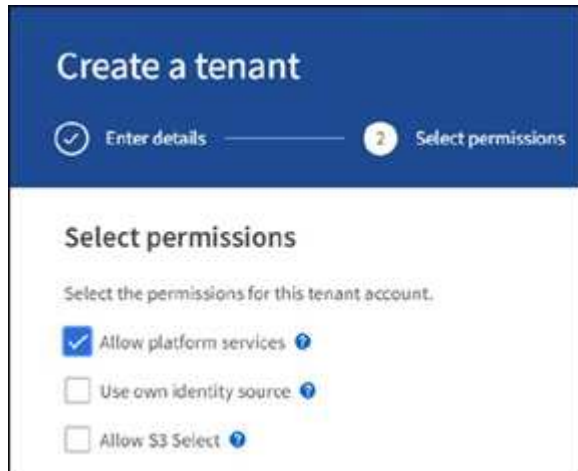
Il presente documento costituisce un'integrazione di ["Guida al tenant di StorageGRID 11.6"](#) inoltre, fornisce istruzioni dettagliate ed esempi per la configurazione di endpoint e bucket per i servizi di integrazione della ricerca. Le istruzioni di configurazione di Amazon Web Services (AWS) o on-premise Elasticsearch qui incluse

sono esclusivamente a scopo dimostrativo o di test di base.

Gli utenti devono avere familiarità con Grid Manager, il tenant manager, e avere accesso al browser S3 per eseguire operazioni di caricamento (PUT) e download (GET) di base per il test di integrazione della ricerca StorageGRID.

Creare tenant e abilitare i servizi della piattaforma

1. Creare un tenant S3 utilizzando Grid Manager, immettere un nome visualizzato e selezionare il protocollo S3.
2. Nella pagina Permission, selezionare l'opzione Allow Platform Services (Consenti servizi piattaforma). Se necessario, selezionare altre autorizzazioni.



3. Impostare la password iniziale dell'utente root tenant oppure, se l'opzione identifica federazione è attivata sulla griglia, selezionare il gruppo federated che dispone dell'autorizzazione di accesso root per configurare l'account tenant.
4. Fare clic su Accedi come root e selezionare bucket: Crea e gestisci bucket.

Viene visualizzata la pagina del tenant manager.

5. Da Tenant Manager, selezionare My Access Keys (chiavi di accesso personali) per creare e scaricare la chiave di accesso S3 per i test successivi.

Cerca servizi di integrazione con Amazon OpenSearch

Configurazione del servizio Amazon OpenSearch (precedentemente chiamato Elasticsearch)

Utilizzare questa procedura per una configurazione rapida e semplice del servizio OpenSearch solo a scopo di test/demo. Se si utilizza on-premise Elasticsearch per i servizi di integrazione della ricerca, consultare la sezione [Cerca servizi di integrazione con Elasticsearch on premise](#).



Per iscriversi al servizio OpenSearch, è necessario disporre di un account di accesso alla console AWS valido, di una chiave di accesso, di una chiave di accesso segreta e dell'autorizzazione.

1. Creare un nuovo dominio utilizzando le istruzioni fornite da "[Guida introduttiva al servizio AWS OpenSearch](#)", ad eccezione di:

- Fase 4. Nome di dominio: Sgdemo
- Fase 10. Controllo degli accessi dettagliato: Deselezionare l'opzione Enable fine-Grained Access Control (attiva controllo degli accessi con grana fine).
- Fase 12. Access policy (criterio di accesso): Selezionare Configure Level Access Policy (Configura policy di accesso a livello), selezionare la scheda JSON per modificare la policy di accesso utilizzando il seguente esempio:
 - Sostituire il testo evidenziato con il proprio ID AWS Identity and Access Management (IAM) e il proprio nome utente.
 - Sostituire il testo evidenziato (l'indirizzo IP) con l'indirizzo IP pubblico del computer locale utilizzato per accedere alla console AWS.
 - Aprire una scheda del browser in "<https://checkip.amazonaws.com>" Per trovare l'IP pubblico.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam:: nnnnnn:user/xyzabc",
      },
      "Action": "es:*",
      "Resource": "arn:aws:es:us-east-1:nnnnnn:domain/sgdemo/*"
    },
    {
      "Effect": "Allow",
      "Principal": { "AWS": "*" },
      "Action": [
        "es:ESHttp*"
      ],
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": [ "nnn.nnn.nn.n/nn" ]
        }
      },
      "Resource": "arn:aws:es:us-east-1:nnnnnn:domain/sgdemo/*"
    }
  ]
}
```

Fine-grained access control

Fine-grained access control provides numerous features to help you keep your data secure. Features include document-level security, field-level security, read-only users, and OpenSearch Dashboards/Kibana tenants. Fine-grained access control requires a master user. [Learn more](#)



☐ Enable fine-grained access control

SAML authentication for OpenSearch Dashboards/Kibana

SAML authentication lets you use your existing identity provider for single sign-on for OpenSearch Dashboards/Kibana. [Learn more](#)



☐ Prepare SAML authentication

To use SAML authentication, you must first enable fine-grained access control.

Amazon Cognito authentication

Enable to use Amazon Cognito authentication for OpenSearch Dashboards/Kibana. Amazon Cognito supports a variety of identity providers for username-password authentication. [Learn more](#)



☐ Enable Amazon Cognito authentication

Access policy

Access policies control whether a request is accepted or rejected when it reaches the Amazon OpenSearch Service domain. If you specify an account, user, or role in this policy, you must sign your requests. [Learn more](#)



Domain access policy

- ☐ Only use fine-grained access control
Allow open access to the domain.
- ☐ Do not set domain level access policy
All requests to the domain will be denied.
- ☒ Configure domain level access policy

Visual editor

JSON

Import policy

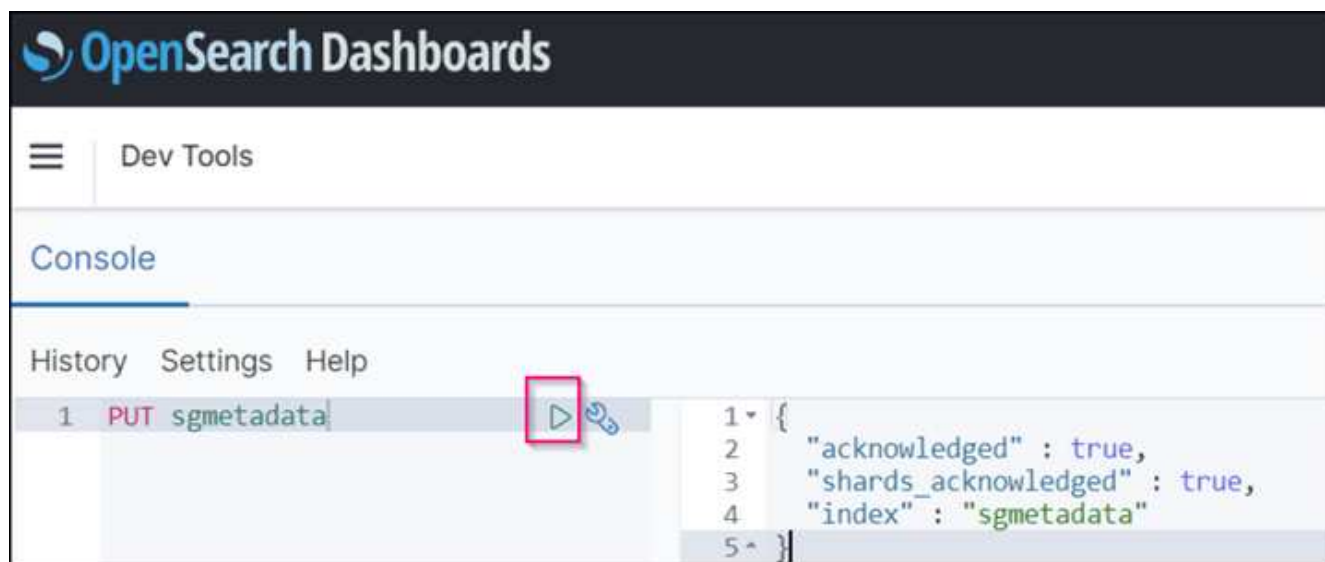
Access policy

```
3+  "Statement": [  
4+  {  
5+    "Effect": "Allow",  
6+    "Principal": {  
7+      "AWS": "arn:aws:iam::123456789012:user/ashley"  
8+    },  
9+    "Action": "es:*",  
10+   "Resource": "arn:aws:es:us-east-1:123456789012:domain/sgdemo/*"  
11+ },  
12+ {  
13+   "Effect": "Allow",  
14+   "Principal": {  
15+     "AWS": "*"   
16+   },  
17+   "Action": [  
18+     "es:ESHttp*"   
19+   ],  
20+   "Condition": {  
21+     "IpAddress": {  
22+       "aws:SourceIp": [  
23+         "216.24.24.24/24"  
24+       ]  
25+     }  
26+   },  
27+   "Resource": "arn:aws:es:us-east-1:123456789012:domain/sgdemo/*"  
28+ }
```

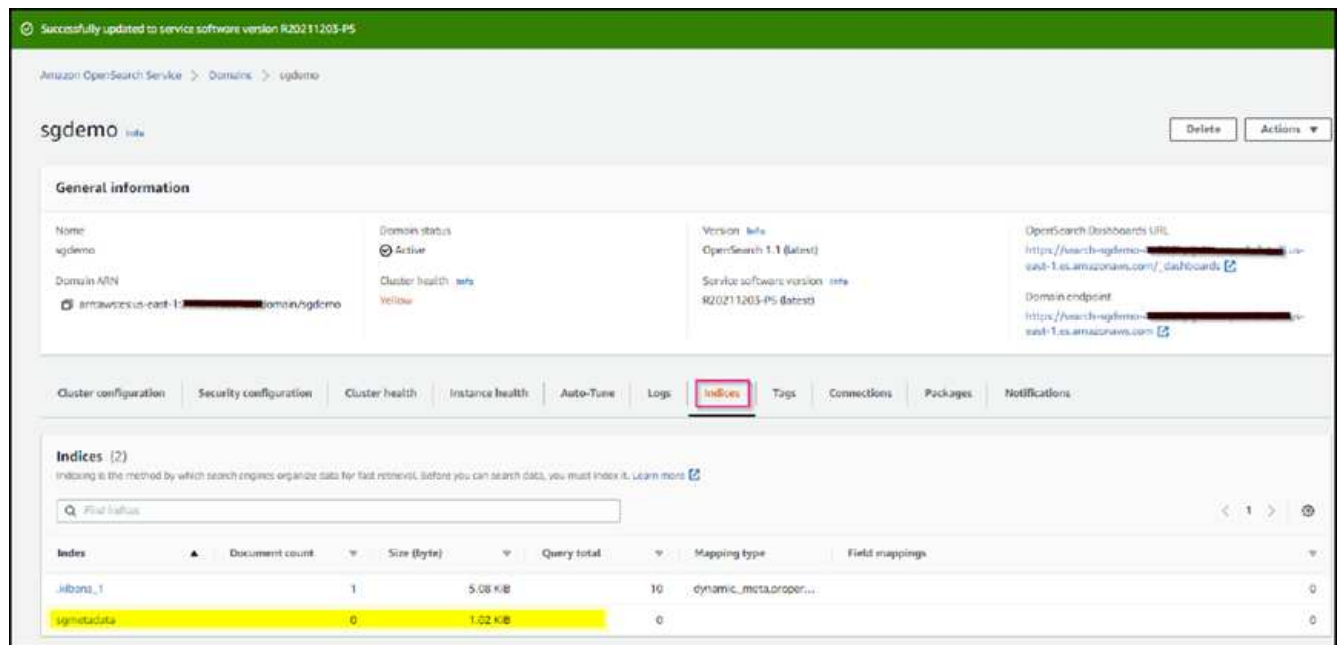
2. Attendere da 15 a 20 minuti per attivare il dominio.



3. Fare clic su OpenSearch Dashboards URL (URL dashboard OpenSearch) per aprire il dominio in una nuova scheda e accedere alla dashboard. Se viene visualizzato un errore di accesso negato, verificare che l'indirizzo IP di origine del criterio di accesso sia impostato correttamente sull'IP pubblico del computer per consentire l'accesso alla dashboard del dominio.
4. Nella pagina di benvenuto della dashboard, selezionare Esplora da solo. Dal menu, selezionare Management (Gestione) → Dev Tools (Strumenti di sviluppo)
5. In Strumenti di sviluppo → Console, immettere `PUT <index>` Dove si utilizza l'indice per memorizzare i metadati degli oggetti StorageGRID. Nell'esempio seguente viene utilizzato il nome dell'indice "sgmetadata". Fare clic sul piccolo simbolo del triangolo per eseguire IL comando PUT. Il risultato previsto viene visualizzato sul pannello di destra, come mostrato nella seguente schermata di esempio.



6. Verificare che l'indice sia visibile dall'interfaccia utente di Amazon OpenSearch in `sgdomain > indici`.



Configurazione degli endpoint dei servizi della piattaforma

Per configurare gli endpoint dei servizi della piattaforma, attenersi alla seguente procedura:

1. In Tenant Manager, andare a STORAGE(S3) > Platform Services Endpoint.
2. Fare clic su Create Endpoint (Crea endpoint), immettere quanto segue, quindi fare clic su Continue (continua):
 - Esempio di nome visualizzato `aws-opensearch`
 - L'endpoint di dominio nella schermata di esempio nella fase 2 della procedura precedente nel campo URI.
 - Il dominio ARN utilizzato nella fase 2 della procedura precedente nel campo URN e aggiungere `/<index>/_doc` Alla fine di ARN.

In questo esempio, URN diventa `arn:aws:es:us-east-1:211234567890:domain/sgdemo/sgmedata/_doc`.

Create endpoint

1

Enter details

2

Select authentication type
Optional

3

Verify server
Optional

Enter endpoint details

Enter the endpoint's display name, URI, and URN.

Display name

aws-opensearch

URI

https://search-sgdemo-4[REDACTED].us-east-1.amazonaws.com

URN

sgdemo:us-east-1:2[REDACTED];domain/sgdemo/sgmetadata/_doc

Cancel

Continue

- 1 Enter details ————— 2 Select authentication type Optional ————— 3 Verify server Optional

Enter endpoint details

Enter the endpoint's display name, URI, and URN.

Display name

aws-opensearch

URI

[https://search-sgdemo-4\[REDACTED\].us-east-1.elb.amazonaws.com/](https://search-sgdemo-4[REDACTED].us-east-1.elb.amazonaws.com/)

URN

```
s;es:us-east-1:2[REDACTED]:domain/sgdemo/sgmetadata/_doc
```

Cancel

Continue

3. Per accedere a Amazon OpenSearch sgdomain, scegli Access Key come tipo di autenticazione, quindi inserisci la chiave di accesso Amazon S3 e la chiave segreta. Per passare alla pagina successiva, fare clic su Continue (continua).

Create endpoint

✓ Enter details

2 Select authentication type Optional

✓ Verify server Optional

Authentication type ?

Select the method used to authenticate connections to the endpoint.

Access Key

Access key ID ?

AKIA[REDACTED]UWO

Secret access key ?

[REDACTED]

Previous

Continue

- Per verificare l'endpoint, selezionare Use Operating System CA Certificate and Test (Usa certificato CA del sistema operativo e test) e Create Endpoint (Crea endpoint). Se la verifica ha esito positivo, viene visualizzata una schermata dell'endpoint simile alla seguente figura. Se la verifica non riesce, verificare che l'URN includa `/<index>/_doc` Alla fine del percorso, la chiave di accesso AWS e la chiave segreta sono corrette.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

1 endpoint Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name ?	Last error ?	Type ?	URI ?	URN ?
<input type="checkbox"/>	aws-opensearch		Search	https://search-sgdemo-1-2021-11-10-12-34-us-east-1.es.amazonaws.com/	arn:aws:es:us-east-1:2021-11-10-12-34-domain/sgdemo/sgmetadata/_doc

Cerca servizi di integrazione con Elasticsearch on premise

Configurazione di Elasticsearch on premise

Questa procedura è per una rapida configurazione di on premise Elasticsearch e Kibana utilizzando docker solo a scopo di test. Se il server Elasticsearch e Kibana esiste già, passare alla fase 5.

1. Seguire questa procedura "[Procedura di installazione di Docker](#)" per installare docker. Utilizziamo il "[Procedura di installazione di CentOS Docker](#)" in questa configurazione.

```
sudo yum install -y yum-utils
sudo yum-config-manager --add-repo
https://download.docker.com/linux/centos/docker-ce.repo
sudo yum install docker-ce docker-ce-cli containerd.io
sudo systemctl start docker
```

- Per avviare docker dopo il riavvio, immettere quanto segue:

```
sudo systemctl enable docker
```

- Impostare `vm.max_map_count` valore 262144:

```
sysctl -w vm.max_map_count=262144
```

- Per mantenere l'impostazione dopo il riavvio, immettere quanto segue:

```
echo 'vm.max_map_count=262144' >> /etc/sysctl.conf
```

2. Seguire la "[Elasticsearch Guida introduttiva](#)" Sezione autogestito per installare ed eseguire il docker Elasticsearch e Kibana. In questo esempio, è stata installata la versione 8.1.



Annotare il nome utente/password e il token creati da Elasticsearch, necessari per avviare l'autenticazione dell'interfaccia utente Kibana e dell'endpoint della piattaforma StorageGRID.

Install and run Elasticsearch

1. Install and start [Docker Desktop](#).
2. Run:

```
docker network create elastic
docker pull docker.elastic.co/elasticsearch/elasticsearch:8.1.0
docker run --name es-node01 --net elastic -p 9200:9200 -p 9300:9300 -it
```

When you start Elasticsearch for the first time, the following security configuration occurs automatically:

- [Certificates and keys](#) are generated for the transport and HTTP layers.
- The Transport Layer Security (TLS) configuration settings are written to `elasticsearch.yml`.
- A password is generated for the `elastic` user.
- An enrollment token is generated for Kibana.



You might need to scroll back a bit in the terminal to view the password and enrollment token.

3. Copy the generated password and enrollment token and save them in a secure location. These values are shown only when you start Elasticsearch for the first time. You'll use these to enroll Kibana with your Elasticsearch cluster and log in.



If you need to reset the password for the `elastic` user or other built-in users, run the [elasticsearch-reset-password](#) tool. To generate new enrollment tokens for Kibana or Elasticsearch nodes, run the [elasticsearch-create-enrollment-token](#) tool. These tools are available in the Elasticsearch `bin` directory.

Install and run Kibana

To analyze, visualize, and manage Elasticsearch data using an intuitive UI, install Kibana.

1. In a new terminal session, run:

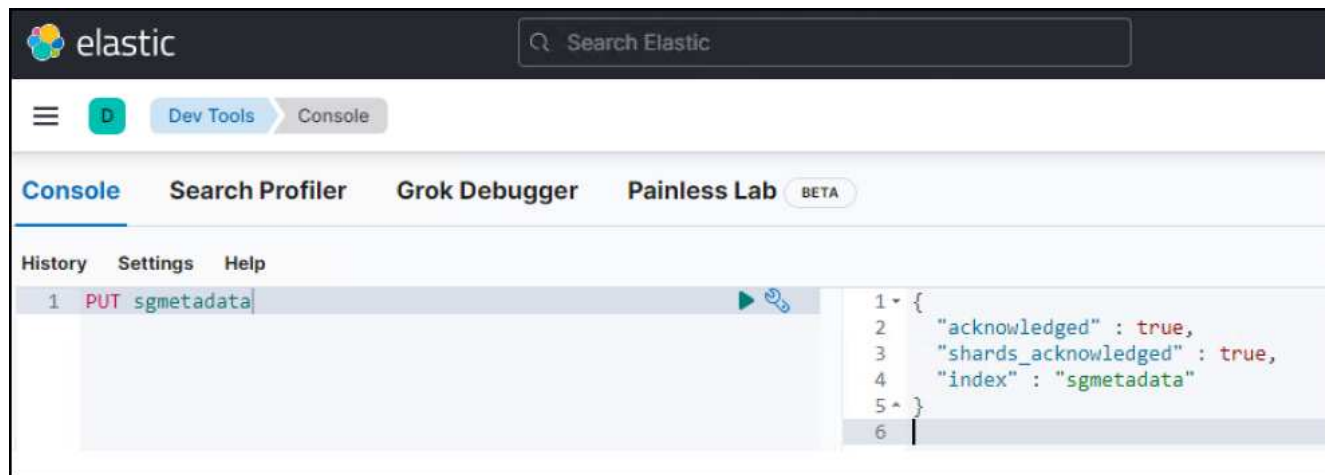
```
docker pull docker.elastic.co/kibana/kibana:8.1.0
docker run --name kib-01 --net elastic -p 5601:5601 docker.elastic.co/k
```

When you start Kibana, a unique link is output to your terminal.

2. To access Kibana, click the generated link in your terminal.

- a. In your browser, paste the enrollment token that you copied and click the button to connect your Kibana instance with Elasticsearch.
- b. Log in to Kibana as the `elastic` user with the password that was generated when you started Elasticsearch.

- Una volta avviato il container Kibana docker, viene visualizzato il link URL `https://0.0.0.0:5601` viene visualizzato nella console. Sostituire 0.0.0.0 con l'indirizzo IP del server nell'URL.
- Accedere all'interfaccia utente di Kibana utilizzando il nome utente `elastic` E la password generata da Elastic nel passaggio precedente.
- Per il primo accesso, nella pagina di benvenuto della dashboard, selezionare Esplora da solo. Dal menu, selezionare Management (Gestione) > Dev Tools (Strumenti di sviluppo).
- Nella schermata Console di Dev Tools, immettere `PUT <index>` Dove si utilizza questo indice per memorizzare i metadati degli oggetti StorageGRID. Utilizziamo il nome dell'indice `sgmetadata` in questo esempio. Fare clic sul piccolo simbolo del triangolo per eseguire IL comando PUT. Il risultato previsto viene visualizzato sul pannello di destra, come mostrato nella seguente schermata di esempio.



Configurazione degli endpoint dei servizi della piattaforma

Per configurare gli endpoint per i servizi della piattaforma, attenersi alla seguente procedura:

- In Tenant Manager, andare a STORAGE(S3) > Platform Services Endpoint
- Fare clic su Create Endpoint (Crea endpoint), immettere quanto segue, quindi fare clic su Continue (continua):
 - Esempio di nome visualizzato: `elasticsearch`
 - URI: `https://<elasticsearch-server-ip or hostname>:9200`
 - URN: `urn:<something>:es:::<some-unique-text>/<index-name>/_doc` Dove index-name è il nome utilizzato sulla console Kibana. Esempio:
`urn:local:es:::sgmd/sgmetadata/_doc`

Create endpoint


1 Enter details


2 Select authentication type
Optional


3 Verify server
Optional

Enter endpoint details

Enter the endpoint's display name, URI, and URN.

Display name 

URI 


URN 


[Cancel](#)[Continue](#)


3. Selezionare HTTP di base come tipo di autenticazione, quindi immettere il nome utente `elastic` e la password generata dal processo di installazione di Elasticsearch. Per passare alla pagina successiva, fare clic su Continue (continua).


Authentication type

Select the method used to authenticate connections to the endpoint.

Basic HTTP 

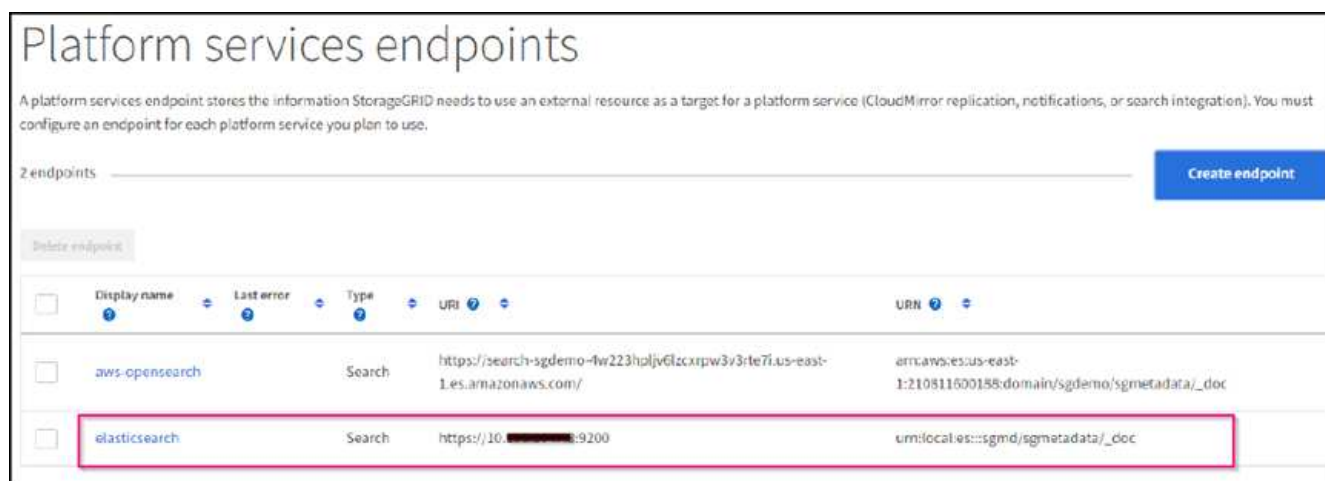
Username 

Password 

..... 

[Previous](#)[Continue](#)

4. Selezionare non verificare certificato e test e Crea endpoint per verificare l'endpoint. Se la verifica ha esito positivo, viene visualizzata una schermata dell'endpoint simile alla seguente schermata. Se la verifica non riesce, verificare che le voci URN, URI e nome utente/password siano corrette.



Configurazione del servizio di integrazione della ricerca nel bucket

Una volta creato l'endpoint del servizio della piattaforma, il passaggio successivo consiste nel configurare questo servizio a livello di bucket per inviare i metadati dell'oggetto all'endpoint definito ogni volta che un oggetto viene creato, cancellato o i relativi metadati o tag vengono aggiornati.

È possibile configurare l'integrazione della ricerca utilizzando Tenant Manager per applicare un XML di configurazione StorageGRID personalizzato a un bucket come segue:

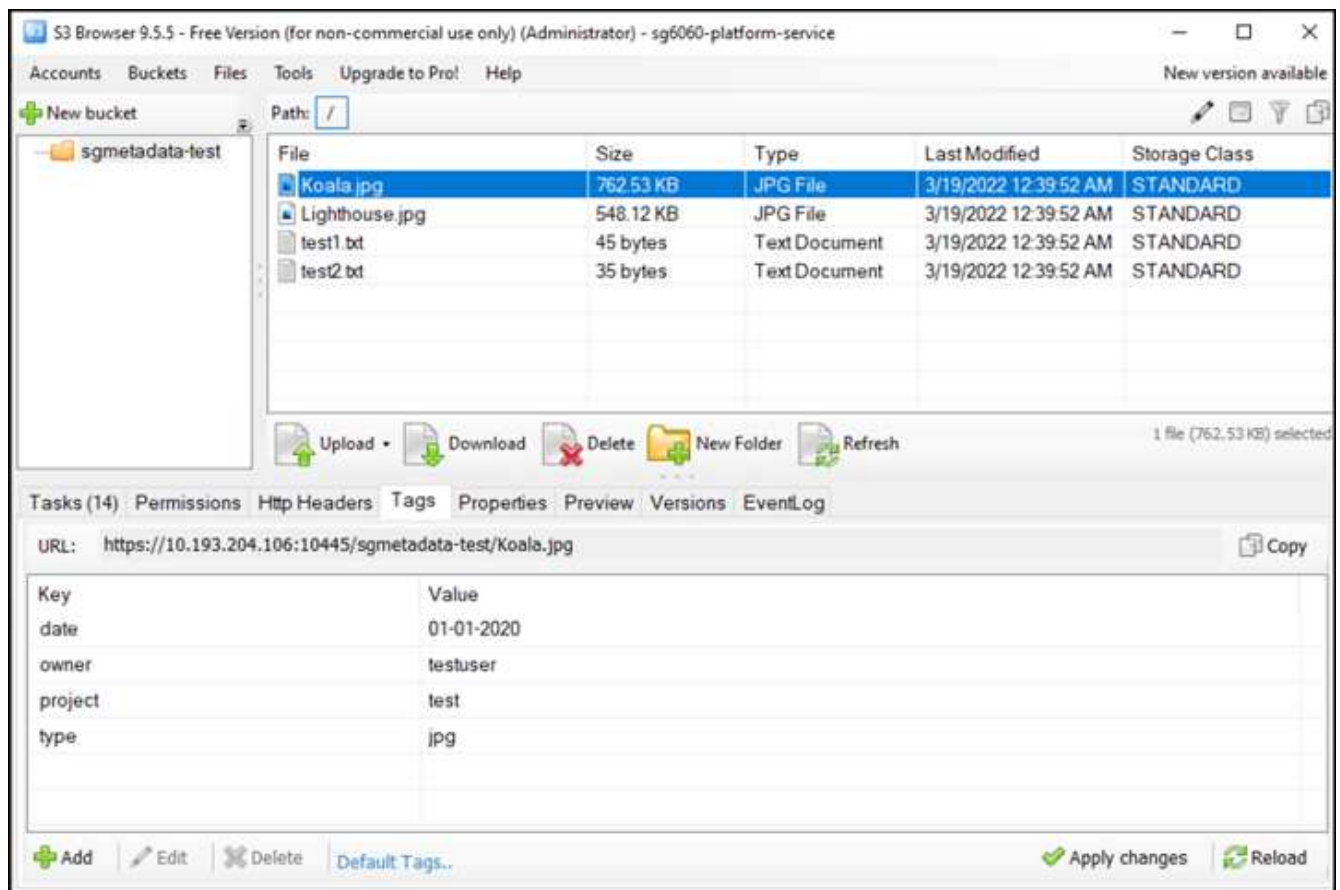
1. In Tenant Manager, andare a STORAGE(S3) > Bucket
2. Fare clic su Create bucket (Crea bucket), inserire il nome del bucket (ad esempio, sgmetadata-test) e accettare l'impostazione predefinita us-east-1 regione.
3. Fare clic su continua > Crea bucket.
4. Per visualizzare la pagina Panoramica del bucket, fare clic sul nome del bucket, quindi selezionare Platform Services (servizi piattaforma).
5. Selezionare la finestra di dialogo Enable Search Integration (attiva integrazione ricerca). Nella casella XML fornita, immettere il file XML di configurazione utilizzando questa sintassi.

L'URN evidenziato deve corrispondere all'endpoint dei servizi della piattaforma definito dall'utente. È possibile aprire un'altra scheda del browser per accedere a Tenant Manager e copiare l'URN dall'endpoint dei servizi della piattaforma definito.

In questo esempio, non abbiamo utilizzato alcun prefisso, il che significa che i metadati per ogni oggetto in questo bucket vengono inviati all'endpoint Elasticsearch definito in precedenza.

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn> urn:local:es:::sgmd/sgmetadata/_doc</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

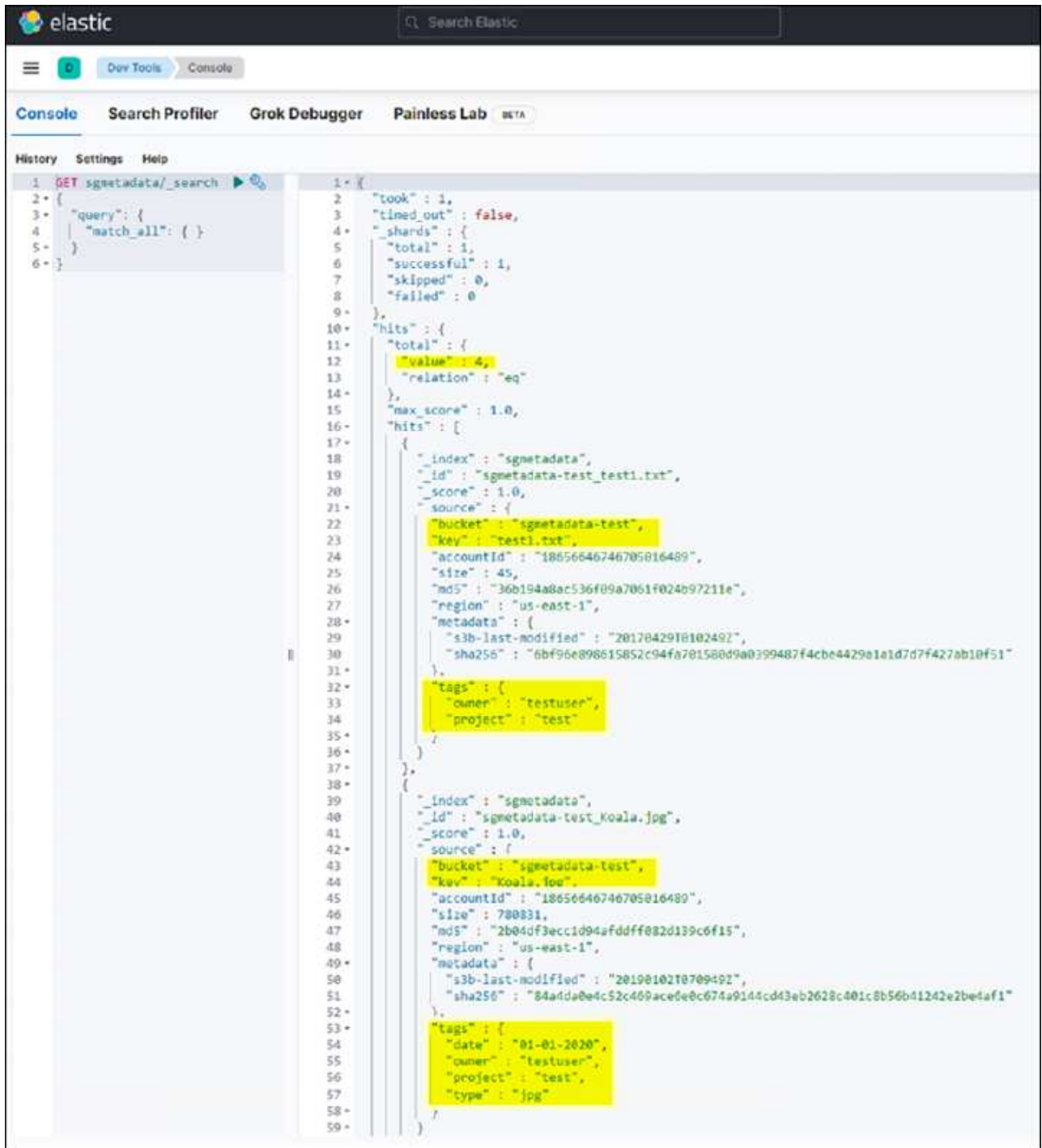
6. Utilizzare S3 browser per connettersi a StorageGRID con la chiave di accesso/segreto del tenant e caricare gli oggetti di test in `sgmetadata-test` bucket e aggiunta di tag o metadati personalizzati agli oggetti.



7. Utilizzare l'interfaccia utente di Kibana per verificare che i metadati dell'oggetto siano stati caricati nell'indice di `sgmetadata`.
 - a. Dal menu, selezionare Management (Gestione) > Dev Tools (Strumenti di sviluppo).
 - b. Incollare la query di esempio nel pannello della console a sinistra e fare clic sul simbolo del triangolo per eseguirla.

Il risultato dell'esempio di query 1 nella seguente schermata di esempio mostra quattro record. Questo corrisponde al numero di oggetti nel bucket.


```
GET sgmetadata/_search
{
  "query": {
    "match_all": { }
  }
}
```



The screenshot shows the Elastic Search console interface. The left sidebar contains navigation links: History, Settings, and Help. The main area is divided into two panels. The left panel shows the query being executed: `GET sgmetadata/_search` with a query object containing `"match_all": { }`. The right panel displays the JSON response from the search engine. The response includes metadata such as `"took": 1`, `"timed_out": false`, and `"_shards": { "total": 1, "successful": 1, "skipped": 0, "failed": 0 }`. The `"hits"` section contains two records. The first record is for a file named `test1.txt` with a score of 1.0. It includes fields for `bucket`, `key`, `accountId`, `size`, `md5`, `region`, `metadata` (with `s3b-last-modified` and `sha256`), and `tags` (with `owner` and `project`). The second record is for a file named `test_Koala.jpg` with a score of 1.0, following a similar structure but with a `type` tag set to `"jpg"`.

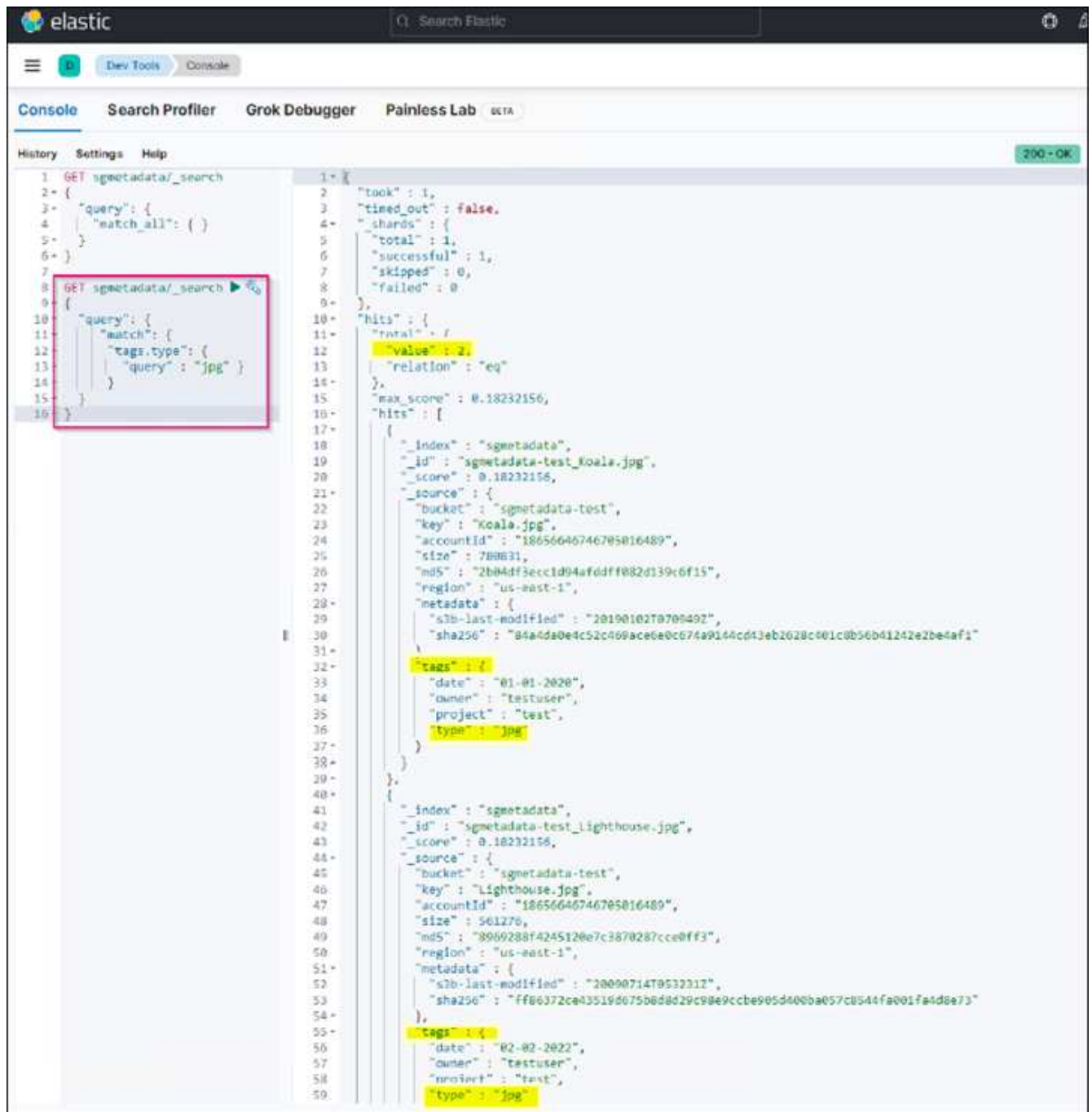
```
1 GET sgmetadata/_search
2 {
3   "query": {
4     "match_all": { }
5   }
6 }

1 {
2   "took": 1,
3   "timed_out": false,
4   "_shards": {
5     "total": 1,
6     "successful": 1,
7     "skipped": 0,
8     "failed": 0
9   },
10  "hits": {
11    "total": {
12      "value": 4,
13      "relation": "eq"
14    },
15    "max_score": 1.0,
16    "hits": [
17      {
18        "_index": "sgmetadata",
19        "_id": "sgmetadata-test_test1.txt",
20        "_score": 1.0,
21        "_source": {
22          "bucket": "sgmetadata-test",
23          "key": "test1.txt",
24          "accountId": "18656646746705016489",
25          "size": 45,
26          "md5": "36b194a8ac536f09a7061f024b97211e",
27          "region": "us-east-1",
28          "metadata": {
29            "s3b-last-modified": "20170429T010249Z",
30            "sha256": "6bf95e898615852c94fa701580d9a0399487f4cbe4429e1a1d7d7f4270b10f51"
31          },
32          "tags": {
33            "owner": "testuser",
34            "project": "test"
35          }
36        }
37      },
38      {
39        "_index": "sgmetadata",
40        "_id": "sgmetadata-test_Koala.jpg",
41        "_score": 1.0,
42        "_source": {
43          "bucket": "sgmetadata-test",
44          "key": "Koala.jpg",
45          "accountId": "18656646746705016489",
46          "size": 780831,
47          "md5": "2b04df3ecc1d94afddff082d139c6f15",
48          "region": "us-east-1",
49          "metadata": {
50            "s3b-last-modified": "20190102T070949Z",
51            "sha256": "84adda0e4c52c409ace6e0c674a9144cd43eb2628c401c8b56b41242e2be4af1"
52          },
53          "tags": {
54            "date": "01-01-2020",
55            "owner": "testuser",
56            "project": "test",
57            "type": "jpg"
58          }
59        }
60      }
61    ]
62  }
63 }
```

Il risultato dell'esempio di query 2 nella seguente schermata mostra due record con il tipo di tag jpg.


```
GET sgmetadata/_search
{
  "query": {
    "match": {
      "tags.type": {
        "query" : "jpg" }
      }
    }
  }
}
```

+



The screenshot shows the Elastic Search Console interface. The left pane displays the search query: `GET sgmetadata/_search` with a `match` query on `tags.type` for the value `jpg`. The right pane shows the search results, which are two documents. The first document is for `sgmetadata-test_koala.jpg` and the second is for `sgmetadata-test_lighthouse.jpg`. Both documents have a score of `0.18232156` and contain metadata such as `bucket`, `key`, `accountId`, `size`, `md5`, `region`, `metadata`, and `tags`.

```
1 GET sgmetadata/_search
2 {
3   "query": {
4     "match": {
5       "tags.type": {
6         "query" : "jpg" }
7       }
8     }
9   }
10 }
```

```
1 {
2   "took" : 1,
3   "timed_out" : false,
4   "shards" : {
5     "total" : 1,
6     "successful" : 1,
7     "skipped" : 0,
8     "failed" : 0
9   },
10  "hits" : {
11    "total" : 2,
12    "value" : 2,
13    "relation" : "eq"
14  },
15  "max_score" : 0.18232156,
16  "hits" : [
17    {
18      "_index" : "sgmetadata",
19      "_id" : "sgmetadata-test_koala.jpg",
20      "_score" : 0.18232156,
21      "_source" : {
22        "bucket" : "sgmetadata-test",
23        "key" : "Koala.jpg",
24        "accountId" : "18656646746705016489",
25        "size" : 788631,
26        "md5" : "2b04df3ecc1d94afddff082d139c6f15",
27        "region" : "us-east-1",
28        "metadata" : {
29          "slb-last-modified" : "20190102T070949Z",
30          "sha256" : "84a4da0e4c52c409ace6a0c674a9144cd43eb2628c001c0b56b41242e2be4af1"
31        },
32        "tags" : {
33          "date" : "01-01-2020",
34          "owner" : "testuser",
35          "project" : "test",
36          "type" : "jpg"
37        }
38      }
39    },
40    {
41      "_index" : "sgmetadata",
42      "_id" : "sgmetadata-test_lighthouse.jpg",
43      "_score" : 0.18232156,
44      "_source" : {
45        "bucket" : "sgmetadata-test",
46        "key" : "Lighthouse.jpg",
47        "accountId" : "18656646746705016489",
48        "size" : 561276,
49        "md5" : "8969288f4245120e7c3870287cce0ff3",
50        "region" : "us-east-1",
51        "metadata" : {
52          "slb-last-modified" : "20090714T053221Z",
53          "sha256" : "ff06372ca43519d075b0d8d29c98e9ccbe905d400ba057c0544fa001fa4d0e73"
54        },
55        "tags" : {
56          "date" : "02-02-2022",
57          "owner" : "testuser",
58          "project" : "test",
59          "type" : "jpg"
60        }
61      }
62    }
63  ]
64 }
```

Dove trovare ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti e/o siti Web:

- ["Cosa sono i servizi della piattaforma"](#)
- ["Documentazione di StorageGRID 11.6"](#)

Di Angela Cheng

Clone del nodo

Considerazioni e performance sui cloni dei nodi.

Considerazioni sui cloni dei nodi

Il clone del nodo può essere un metodo più rapido per sostituire i nodi appliance esistenti per un aggiornamento tecnico, aumentare la capacità o aumentare le performance del sistema StorageGRID. Il clone del nodo può essere utile anche per la conversione alla crittografia del nodo con un KMS o per la modifica di un nodo di storage da DDP8 a DDP16.

- La capacità utilizzata del nodo di origine non è rilevante per il tempo richiesto per il completamento del processo di clonazione. Il clone del nodo è una copia completa del nodo che include spazio libero nel nodo.
- Le appliance di origine e di destinazione devono essere della stessa versione PGE
- Il nodo di destinazione deve avere sempre una capacità maggiore rispetto all'origine
 - Assicurarsi che il nuovo dispositivo di destinazione abbia un disco di dimensioni maggiori rispetto a quello di origine
 - Se il dispositivo di destinazione dispone di unità delle stesse dimensioni ed è configurato per il DDP8, è possibile configurare la destinazione per il DDP16. Se l'origine è già configurata per DDP16, non sarà possibile clonare il nodo.
 - Quando si passa dalle appliance SG5660 o SG5760 alle appliance SG6060, tenere presente che le unità SG5x60 dispongono di 60 dischi di capacità, mentre le unità SG6060 ne hanno solo 58.
- Il processo di clonazione del nodo richiede che il nodo di origine sia offline nella griglia per tutta la durata del processo di clonazione. Se un nodo aggiuntivo passa offline durante questo periodo di tempo, i servizi client potrebbero risentire.
- 11,8 e soffietto: Un nodo storage può essere offline solo per 15 giorni. Se la stima del processo di cloning è prossima a 15 giorni o supera i 15 giorni, utilizzare le procedure di espansione e decommissionamento.
 - 11,9: Il limite di 15 giorni è stato rimosso.
- Per un SG6060 o SG6160 con shelf di espansione, è necessario aggiungere al tempo dell'appliance di base il tempo necessario per le dimensioni corrette dello shelf, per ottenere l'intera durata del clone.
- Il numero di volumi in un dispositivo di storage di destinazione deve essere maggiore o uguale al numero di volumi nel nodo di origine. Non è possibile clonare un nodo di origine con volumi di archivi di oggetti 16 (rangedb) in un'appliance di storage di destinazione con volumi di archivi di oggetti 12, anche se l'appliance di destinazione ha una capacità maggiore rispetto al nodo di origine. La maggior parte delle appliance di storage dispone di 16 volumi di archivi di oggetti, ad eccezione dell'appliance di storage SGF6112 che ha solo 12 volumi di archivi di oggetti. Ad esempio, non è possibile clonare da SG5760 a SGF6112.

Stime delle performance dei cloni dei nodi

Le seguenti tabelle contengono stime calcolate per la durata del clone del nodo. Le condizioni variano, pertanto, le voci in **BOLD** potrebbero rischiare di superare il limite di 15 giorni per un nodo inattivo.

DDP8

SG5612/SG5712/SG5812 → QUALSIASI

Velocità dell'interfaccia di rete	Dimensioni dell'unità 4 TB	Dimensioni disco 8 TB	Dimensioni disco 10 TB	12 TB di capacità dell'unità	Dimensioni dell'unità 16 TB	Dimensioni dell'unità 18 TB	Dimensioni dell'unità 22 TB
10 GB	1 giorno	2 giorni	2.5 giorni	3 giorni	4 giorni	4.5 giorni	5.5 giorni
25 GB	1 giorno	2 giorni	2.5 giorni	3 giorni	4 giorni	4.5 giorni	5.5 giorni

SG5660 → SG5760/SG5860

Velocità dell'interfaccia di rete	Dimensioni dell'unità 4 TB	Dimensioni disco 8 TB	Dimensioni disco 10 TB	12 TB di capacità dell'unità	Dimensioni dell'unità 16 TB	Dimensioni dell'unità 18 TB	Dimensioni dell'unità 22 TB
10 GB	3.5 giorni	7 giorni	8.5 giorni	10.5 giorni	13,5 giorni	15,5 giorni	18,5 giorni
25 GB	3.5 giorni	7 giorni	8.5 giorni	10.5 giorni	13,5 giorni	15,5 giorni	18,5 giorni

SG5660 → SG6060/SG6160

Velocità dell'interfaccia di rete	Dimensioni dell'unità 4 TB	Dimensioni disco 8 TB	Dimensioni disco 10 TB	12 TB di capacità dell'unità	Dimensioni dell'unità 16 TB	Dimensioni dell'unità 18 TB	Dimensioni dell'unità 22 TB
10 GB	2.5 giorni	4.5 giorni	5.5 giorni	6.5 giorni	9 giorni	10 giorni	12 giorni
25 GB	2 giorni	4 giorni	5 giorni	6 giorni	8 giorni	9 giorni	10 giorni

SG5760/SG5860 → SG5760/SG5860

Velocità dell'interfaccia di rete	Dimensioni dell'unità 4 TB	Dimensioni disco 8 TB	Dimensioni disco 10 TB	12 TB di capacità dell'unità	Dimensioni dell'unità 16 TB	Dimensioni dell'unità 18 TB	Dimensioni dell'unità 22 TB
10 GB	3.5 giorni	7 giorni	8.5 giorni	10.5 giorni	13,5 giorni	15,5 giorni	18,5 giorni
25 GB	3.5 giorni	7 giorni	8.5 giorni	10.5 giorni	13,5 giorni	15,5 giorni	18,5 giorni

SG5760/SG5860 → SG6060/SG6160

Velocità dell'interfaccia di rete	Dimensioni dell'unità 4 TB	Dimensioni disco 8 TB	Dimensioni disco 10 TB	12 TB di capacità dell'unità	Dimensioni dell'unità 16 TB	Dimensioni dell'unità 18 TB	Dimensioni dell'unità 22 TB
10 GB	2.5 giorni	4.5 giorni	5.5 giorni	6.5 giorni	9 giorni	10 giorni	12 giorni
25 GB	2 giorni	3.5 giorni	4.5 giorni	5.5 giorni	7 giorni	8 giorni	9.5 giorni

SG6060/SG6160 → SG6060/SG6160

Velocità dell'interfaccia di rete	Dimensioni dell'unità 4 TB	Dimensioni disco 8 TB	Dimensioni disco 10 TB	12 TB di capacità dell'unità	Dimensioni dell'unità 16 TB	Dimensioni dell'unità 18 TB	Dimensioni dell'unità 22 TB
10 GB	2.5 giorni	4.5 giorni	5.5 giorni	6.5 giorni	8.5 giorni	9.5 giorni	11.5 giorni
25 GB	2 giorni	3 giorni	4 giorni	4.5 giorni	6 giorni	7 giorni	8.5 giorni

DDP16

SG5760/SG5860 → SG5760/SG5860

Velocità dell'interfaccia di rete	Dimensioni dell'unità 4 TB	Dimensioni disco 8 TB	Dimensioni disco 10 TB	12 TB di capacità dell'unità	Dimensioni dell'unità 16 TB	Dimensioni dell'unità 18 TB	Dimensioni dell'unità 22 TB
10 GB	3.5 giorni	6.5 giorni	8 giorni	9.5 giorni	12,5 giorni	14 giorni	17 giorni
25 GB	3.5 giorni	6.5 giorni	8 giorni	9.5 giorni	12,5 giorni	14 giorni	17 giorni

Velocità dell'interfaccia di rete	Dimensioni dell'unità 4 TB	Dimensioni disco 8 TB	Dimensioni disco 10 TB	12 TB di capacità dell'unità	Dimensioni dell'unità 16 TB	Dimensioni dell'unità 18 TB	Dimensioni dell'unità 22 TB
10 GB	2.5 giorni	5 giorni	6 giorni	7.5 giorni	10 giorni	11 giorni	13 giorni
25 GB	2 giorni	3.5 giorni	4 giorni	5 giorni	6.5 giorni	7 giorni	8.5 giorni

Velocità dell'interfaccia di rete	Dimensioni dell'unità 4 TB	Dimensioni disco 8 TB	Dimensioni disco 10 TB	12 TB di capacità dell'unità	Dimensioni dell'unità 16 TB	Dimensioni dell'unità 18 TB	Dimensioni dell'unità 22 TB
10 GB	3 giorni	5 giorni	6 giorni	7 giorni	9.5 giorni	10.5 giorni	13 giorni
25 GB	2 giorni	3.5 giorni	4.5 giorni	5 giorni	7 giorni	7.5 giorni	9 giorni

Shelf di espansione (aggiunta a oltre SG6060 TB/SG6160 TB per ogni shelf sull'appliance di origine)

Velocità dell'interfaccia di rete	Dimensioni dell'unità 4 TB	Dimensioni disco 8 TB	Dimensioni disco 10 TB	12 TB di capacità dell'unità	Dimensioni dell'unità 16 TB	Dimensioni dell'unità 18 TB	Dimensioni dell'unità 22 TB
10 GB	3.5 giorni	5 giorni	6 giorni	7 giorni	9.5 giorni	10.5 giorni	12 giorni
25 GB	2 giorni	3 giorni	4 giorni	4.5 giorni	6 giorni	7 giorni	8.5 giorni

Di Aron Klein

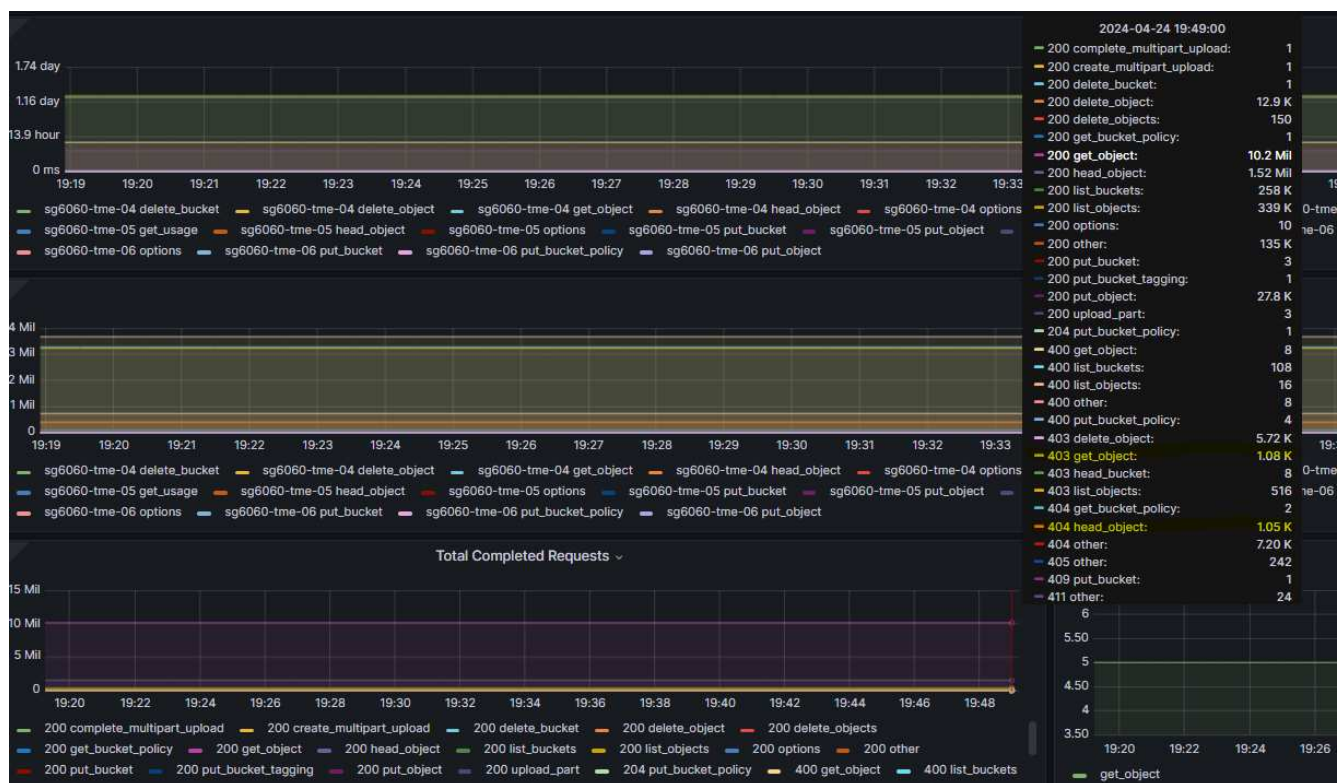
Procedura di trasferimento del sito a griglia e di modifica della rete a livello di sito

Questa guida descrive la preparazione e la procedura per il trasferimento del sito StorageGRID in una griglia multisito. È necessario avere una conoscenza completa di questa procedura e pianificare in anticipo per garantire un processo senza problemi e ridurre al minimo le interruzioni per i clienti.

Se è necessario modificare la rete Grid di tutta la griglia, vedere ["Modificare gli indirizzi IP per tutti i nodi nella griglia"](#).

Considerazioni prima del trasferimento del sito

- Lo spostamento del sito deve essere completato e tutti i nodi online entro 15 giorni per evitare la ricostruzione del database Cassandra.
["Recovery Storage Node Down per più di 15 giorni"](#)
- Se una regola ILM delle policy attive utilizza un comportamento di acquisizione rigoroso, considerare la possibilità di cambiarlo in modo da bilanciarlo o in dual commit se il cliente desidera continuare a INSERIRE gli oggetti nel Grid durante il trasferimento del sito.
- Per le appliance storage con 60 dischi o più, non spostare mai lo shelf con i dischi installati. Etichettare ciascuna unità disco e rimuoverla dal contenitore di archiviazione prima di imballarla/spostarla.
- Modifica appliance StorageGRID la rete VLAN può essere eseguita in remoto tramite rete di amministrazione o rete client. Oppure si prevede di essere in loco per eseguire la modifica prima o dopo il trasferimento.
- Verificare se l'applicazione cliente sta utilizzando HEAD o OTTENERE l'oggetto di non esistenza prima di METTERE. In caso affermativo, modificare la coerenza del bucket in strong-site per evitare l'errore HTTP 500. In caso di dubbi, consultare la panoramica S3 grafici Grafana **Grid manager > supporto > metriche**, passare il mouse sul grafico "richiesta totale completata". Se il conteggio è molto elevato di 404 oggetti GET o 404 oggetti Head, probabilmente una o più applicazioni utilizzano l'oggetto Head o Get nonexistence. Il conteggio è cumulativo, passare il mouse su una timeline diversa per vedere la differenza.



Procedura di modifica dell'indirizzo IP della griglia prima del trasferimento del sito

Fasi

- Se la nuova subnet di rete della griglia viene utilizzata nella nuova posizione,
["Aggiungere la subnet all'elenco delle subnet di rete della griglia"](#)
- Accedere al nodo di amministrazione primario, utilizzare change-ip per modificare l'IP della griglia, deve **stage** la modifica prima di arrestare il nodo per il trasferimento.

- a. Selezionare 2 quindi 1 per la modifica dell'IP della griglia

Editing: Node IP/subnet and gateway

Use up arrow to recall a previously typed value, which you can then edit
Use d or 0.0.0.0/0 as the IP/mask to delete the network from the node
Use q to complete the editing session early and return to the previous menu
Press <enter> to use the value shown in square brackets

=====
Site: LONDON
=====

LONDON-ADM1	Grid	IP/mask	[10.45.74.14/26]:	10.45.74.24/26
LONDON-S1	Grid	IP/mask	[10.45.74.16/26]:	10.45.74.26/26
LONDON-S2	Grid	IP/mask	[10.45.74.17/26]:	10.45.74.27/26
LONDON-S3	Grid	IP/mask	[10.45.74.18/26]:	10.45.74.28/26

=====

LONDON-ADM1	Grid	Gateway	[10.45.74.1]:
LONDON-S1	Grid	Gateway	[10.45.74.1]:
LONDON-S2	Grid	Gateway	[10.45.74.1]:
LONDON-S3	Grid	Gateway	[10.45.74.1]:

=====

=====
Site: OXFORD
=====

OXFORD-ADM1	Grid	IP/mask	[10.45.75.14/26]:
OXFORD-S1	Grid	IP/mask	[10.45.75.16/26]:
OXFORD-S2	Grid	IP/mask	[10.45.75.17/26]:
OXFORD-S3	Grid	IP/mask	[10.45.75.18/26]:

=====

OXFORD-ADM1	Grid	Gateway	[10.45.75.1]:
OXFORD-S1	Grid	Gateway	[10.45.75.1]:
OXFORD-S2	Grid	Gateway	[10.45.75.1]:
OXFORD-S3	Grid	Gateway	[10.45.75.1]:

=====

Finished editing. Press Enter to return to menu. █

- b. selezionare 5 per visualizzare le modifiche

=====
Site: LONDON
=====

LONDON-ADM1	Grid	IP	[10.45.74.14/26]:	10.45.74.24/26
LONDON-S1	Grid	IP	[10.45.74.16/26]:	10.45.74.26/26
LONDON-S2	Grid	IP	[10.45.74.17/26]:	10.45.74.27/26
LONDON-S3	Grid	IP	[10.45.74.18/26]:	10.45.74.28/26

Press Enter to continue █

- c. selezionare 10 per convalidare e applicare la modifica.


```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:  SELECT NODES to edit
2:  EDIT IP/mask and gateway
3:  EDIT admin network subnet lists
4:  EDIT grid network subnet list
5:  SHOW changes
6:  SHOW full configuration, with changes highlighted
7:  VALIDATE changes
8:  SAVE changes, so you can resume later
9:  CLEAR all changes, to start fresh
10: APPLY changes to the grid
0:  Exit

Selection: 10
```

d. In questa fase è necessario selezionare **fase**.

```
Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Applying these changes will update the following nodes:

LONDON-ADM1
LONDON-S1
LONDON-S2
LONDON-S3

The following nodes will also require restarting:

LONDON-ADM1
LONDON-S1
LONDON-S2
LONDON-S3

Select one of the following options:

apply:  apply all changes and automatically restart nodes (if necessary)
stage:  stage the changes; no changes will take effect until the nodes are restarted
cancel: do not make any network changes at this time

[apply/stage/cancel]> stage
```

e. Se il nodo di amministrazione primario è incluso nella modifica precedente, immettere **'A'** per riavviare manualmente il nodo di amministrazione primario


```

10.45.74.14 - PuTTY
Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Applying these changes will update the following nodes:

LONDON-ADM1
LONDON-S1
LONDON-S2
LONDON-S3

The following nodes will also require restarting:

LONDON-ADM1
LONDON-S1
LONDON-S2
LONDON-S3

Select one of the following options:

apply: apply all changes and automatically restart nodes (if necessary)
stage: stage the changes; no changes will take effect until the nodes are restarted
cancel: do not make any network changes at this time

[apply/stage/cancel]> stage

Generating new grid networking description file... PASSED.
Running provisioning... PASSED.
Updating network configuration on LONDON-S1... PASSED.
Updating network configuration on LONDON-S2... PASSED.
Updating network configuration on LONDON-S3... PASSED.
Updating network configuration on LONDON-ADM1... PASSED.
Finished staging network changes. You must manually restart these nodes for the changes to take effect:

LONDON-ADM1 (has IP 10.45.74.14 until restart)
LONDON-S1 (has IP 10.45.74.16 until restart)
LONDON-S2 (has IP 10.45.74.17 until restart)
LONDON-S3 (has IP 10.45.74.18 until restart)

Importing bundles... PASSED.
*****
*                               *
*             IMPORTANT         *
*                               *
* A new recovery package has been generated as a result of the *
* configuration change. Select Maintenance > Recovery Package *
* in the Grid Manager to download it.                          *
*                               *
*****

Network Update Complete. Primary admin restart required. Select 'continue' to restart this node immediately, 'abort' to restart manually.
Enter a to abort, c to continue [a/c]>

```

f. Premere invio per tornare al menu precedente e uscire dall'interfaccia change-ip.

```

Network Update Complete. Primary admin restart required. Select 'continue' to restart this node immediately, 'abort' to restart manually.
Enter a to abort, c to continue [a/c]> a
Restart aborted. You must manually restart this node as soon as possible
Press Enter to return to the previous menu.

```

- Da Grid Manager, scaricare il nuovo pacchetto di ripristino. **Grid manager > Maintenance > Recovery package**
- Se è necessario modificare la VLAN sull'appliance StorageGRID, vedere la sezione [Modifica VLAN dell'appliance](#).
- Arrestare tutti i nodi e/o le appliance in sede, etichettare/rimuovere le unità disco se necessario, disimballare, imballare e spostare.
- Se si prevede di modificare l'indirizzo ip della rete amministrativa e/o la VLAN e l'indirizzo ip del client, è possibile eseguire la modifica dopo il trasferimento.

Modifica VLAN dell'appliance

La procedura riportata di seguito presuppone l'accesso remoto alla rete client o di amministrazione dell'appliance StorageGRID per eseguire la modifica in remoto.

Fasi

- Prima di spegnere l'apparecchio, ["impostare l'apparecchio in modalità di manutenzione"](#).

2. Utilizzando un browser per accedere alla GUI del programma di installazione dell'appliance StorageGRID utilizzando <https://<admin-or-client-network-ip>:8443>. Non è possibile utilizzare Grid IP come nuovo Grid IP già in uso dopo l'avvio dell'appliance in modalità di manutenzione.
3. Modificare la VLAN per la rete Grid. Se si accede all'appliance tramite la rete client, non è possibile modificare la VLAN client in questo momento, è possibile modificarla dopo lo spostamento.
4. ssh per l'appliance e spegnere il nodo utilizzando 'hutdown -h now'
5. Dopo che le appliance sono pronte presso il nuovo sito, accedere alla GUI del programma di installazione dell'appliance StorageGRID utilizzando <https://<grid-network-ip>:8443>. Verificare che lo storage sia in uno stato ottimale e la connettività di rete agli altri nodi Grid utilizzando gli strumenti ping/nmap nella GUI.
6. Se si prevede di modificare l'IP della rete client, è possibile modificare la VLAN client in questa fase. La rete client non è pronta finché non si aggiorna l'ip della rete client utilizzando lo strumento change-ip nel passaggio successivo.
7. Uscire dalla modalità di manutenzione. Dal programma di installazione dell'appliance StorageGRID, selezionare **Avanzate** > **Riavvia controller**, quindi selezionare **Riavvia in StorageGRID**.
8. Dopo che tutti i nodi sono attivi e Grid non mostra alcun problema di connettività, utilizzare change-ip per aggiornare la rete di amministrazione dell'appliance e la rete client, se necessario.

Migrazione dello storage a oggetti da ONTAP S3 a StorageGRID

Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID

Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID

Demo sulla migrazione

Questa è una dimostrazione sulla migrazione di utenti e bucket da ONTAP S3 a StorageGRID.

Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID

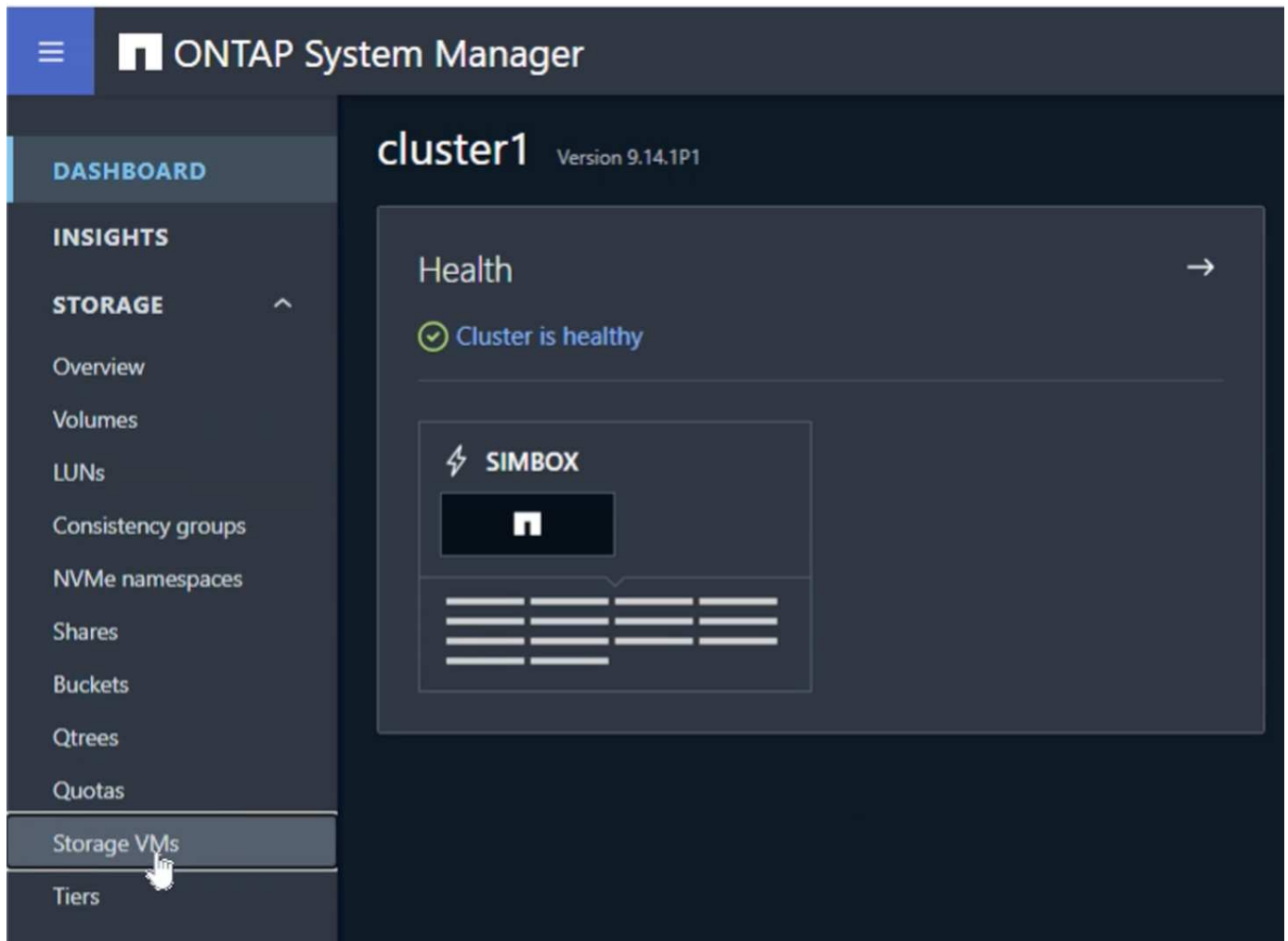
Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID

Preparazione di ONTAP

A scopo dimostrativo creeremo un server per archivio di oggetti SVM, un utente, un gruppo, una policy di gruppo e bucket.

Creare la Storage Virtual Machine

In Gestione sistema di ONTAP, accedere alle VM di archiviazione e aggiungere una nuova VM di archiviazione.



Selezionare le caselle di controllo "Enable" (attiva S3) e "Enable TLS" (attiva TLS) e configurare le porte HTTP(S). Definire l'IP, la subnet mask e definire il gateway e il dominio di broadcast se non si utilizza l'impostazione predefinita o obbligatoria nell'ambiente in uso.

Add storage VM



STORAGE VM NAME

svm_demo

Access protocol

☒ SMB/CIFS, NFS, S3

iSCSI

FC

NVMe

☐ Enable SMB/CIFS

☐ Enable NFS

☒ Enable S3

S3 SERVER NAME

s3portal.demo.netapp.com

☒ Enable TLS

PORT

443

CERTIFICATE

☒ Use system-generated certificate

☐ Use external-CA signed certificate

☐ Use HTTP (non-secure)

PORT

8080

DEFAULT LANGUAGE

c.utf_8

NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

onPrem-01

IP ADDRESS

192.168.0.200

SUBNET MASK

24

GATEWAY

Add optional gateway

BROADCAST DOMAIN AND PORT

Default

Storage VM administration

☐ Enable maximum capacity limit

The maximum capacity that all volumes in this storage VM can allocate. [Learn More](#)

☐ Manage administrator account

Save

Cancel

Durante la creazione della SVM verrà creato un utente. Scaricare i S3 tasti per questo utente e chiudere la finestra.

Added storage VM

STORAGE VM

svm_demo


S3 SERVER NAME

s3portal.demo.netapp.com

User details


USER NAME

sm_s3_user

 The secret key won't be displayed again. Save this key for future use.

ACCESS KEY

34EH21411SMW1YOV3NQY



SECRET KEY

Show secret key



Download

Close

Una volta creata la SVM, edita la SVM e Aggiungi le impostazioni DNS.



Services


NIS



Not configured

Name service switch



Services lookup order 

HOSTS

Files, then DNS

GROUP

Files



NAME MAP

Files

NETGROUP

Files

DNS



Not configured

Definire il nome DNS e l'IP.

The screenshot shows a dark-themed dialog box titled "Add DNS domain" with a close button (X) in the top right corner. The dialog is divided into two sections: "DNS domains" and "Name servers".

DNS domains

A text input field contains the domain "demo.netapp.com". Below the input field is a blue "+ Add" button.

Name servers









A text input field contains the IP address "192.168.0.253". Below the input field is a greyed-out "+ Add" button.

At the bottom right of the dialog, there are two buttons: a blue "Save" button and a greyed-out "Cancel" button. A mouse cursor is visible near the bottom center of the dialog.

Creare un utente SVM S3

Ora possiamo configurare i S3 utenti e il gruppo. Modificare le impostazioni S3.

Protocols

NFS Not configured	 	SMB/CIFS Not configured	 	iSCSI Not configured
NVMe Not configured	 	S3 STATUS ✓ Enabled TLS Disabled HTTP Enabled	 	

Aggiungere un nuovo utente.

Storage VMs

+ Add

More

☒ Name

☒ svm_demo

S3

All settings

Enabled

Server

Edit

FQDN

s3portal.demo.netapp.com

TLS

Disabled

TLS PORT

443

HTTP

Enabled

HTTP PORT

8080

Users

Groups

Policies

+ Add

User name	Access key	Key expiration time
root		-
sm_s3_user	34EH21411SMW1YOV3NQY	Valid forever

Inserire il nome utente e la scadenza della chiave.

Storage VMs

+ Add

More

☒ Name

☒ svm_demo

S3

All settings

Enabled

Server

Edit

FQDN

s3portal.demo.netapp.com

TLS

Disabled

TLS PORT

443

HTTP

Enabled

HTTP PORT

8080

Users

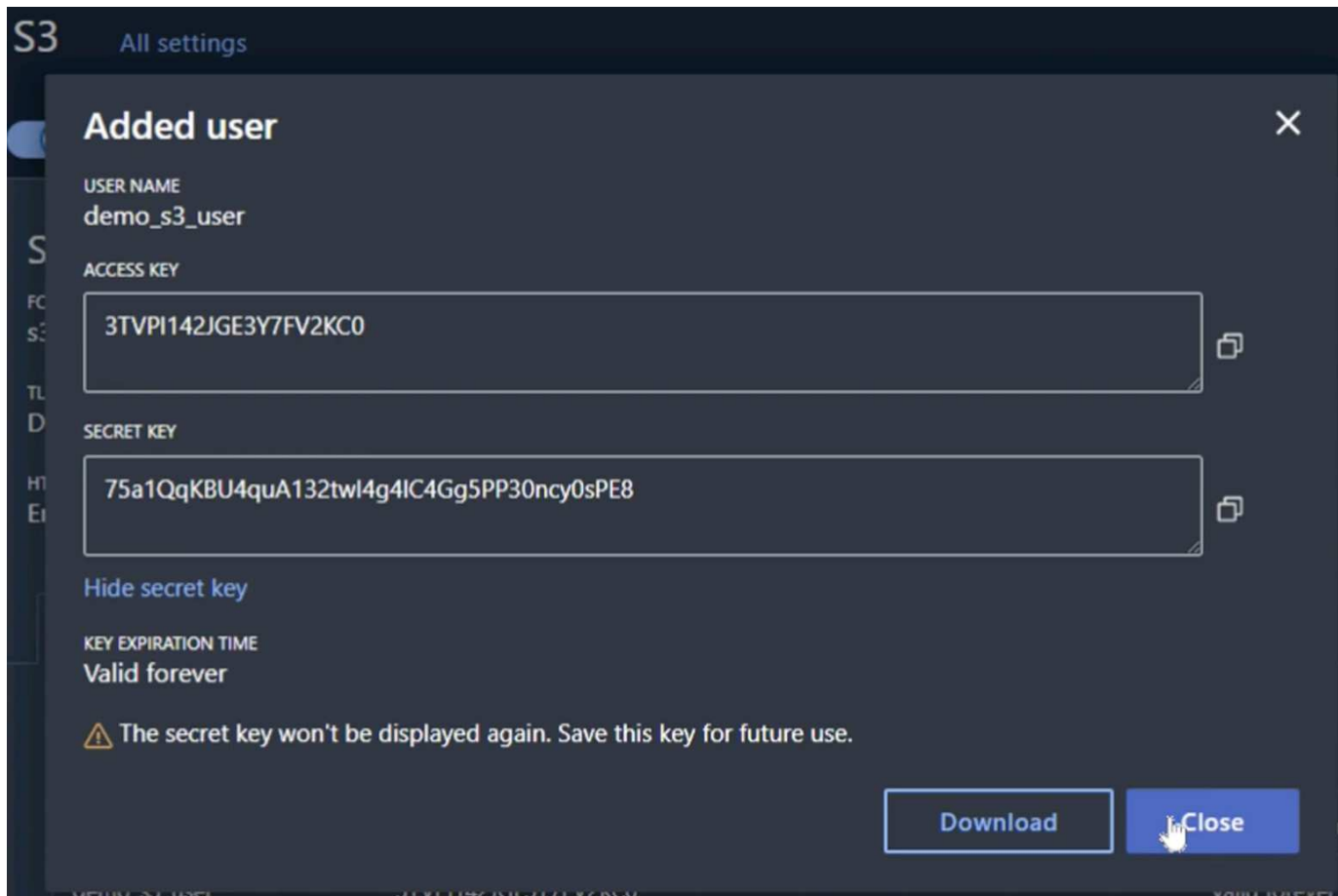
Groups

Policies

+ Add

User name	Access key	Key expiration time
root		-
sm_s3_user	34EH21411SMW1YOV3NQY	Valid forever

Scaricare i S3 tasti per il nuovo utente.



Creare un gruppo SVM S3

Nella scheda Groups (gruppi) delle impostazioni SVM S3, aggiungere un nuovo gruppo con l'utente creato in precedenza e le autorizzazioni FullAccess.

Add group ×

NAME

demo_s3_group

USERS

demo_s3_user ×

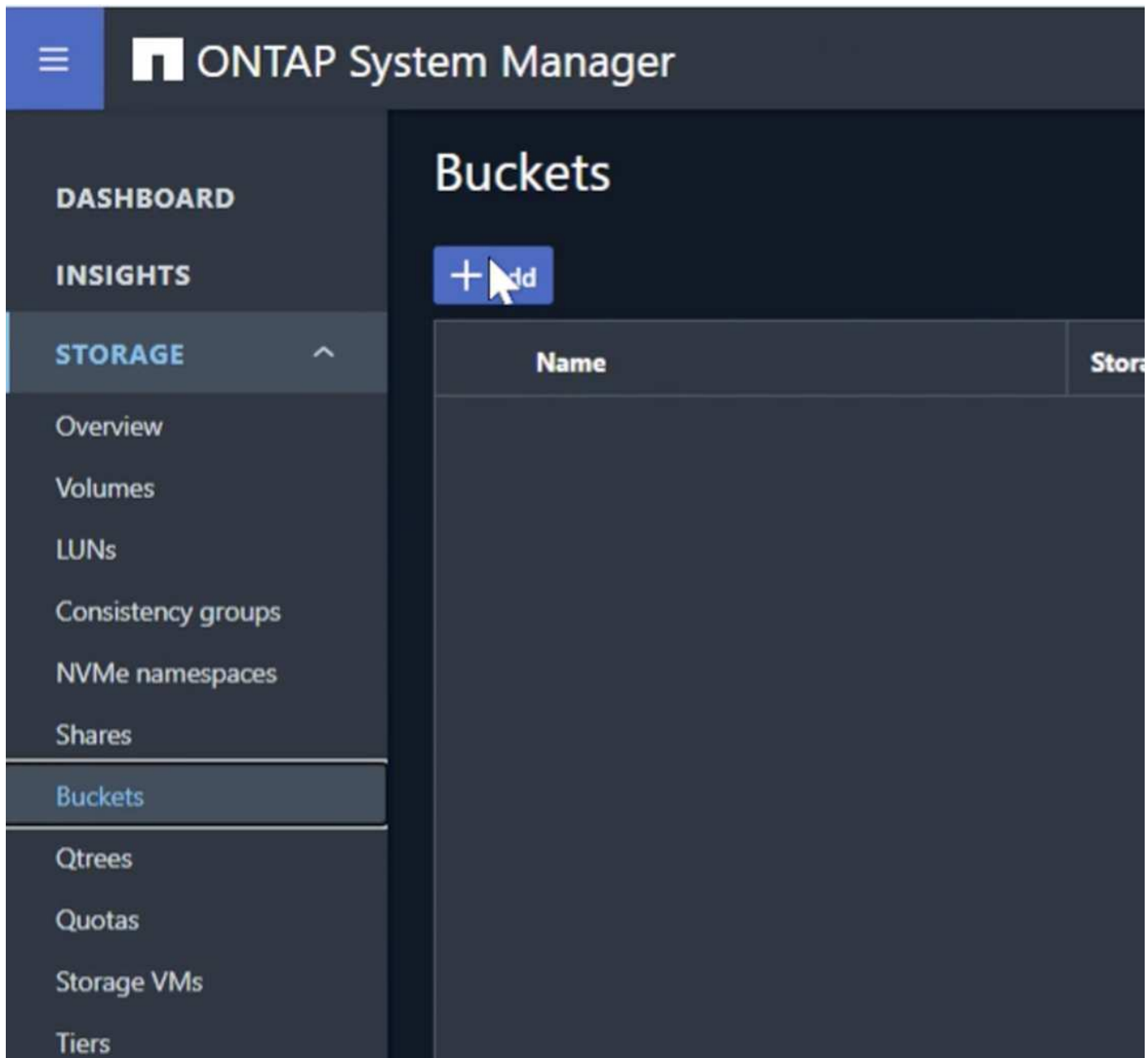
POLICIES

FullAccess ×

Cancel Save

Creare bucket SVM S3

Passare alla sezione benne e fare clic sul pulsante "+Aggiungi".



Immettere un nome, una capacità e deselezionare la casella di controllo "Abilita accesso a ListBucket...", quindi fare clic sul pulsante "altre opzioni".

Add bucket

NAME

bucket

CAPACITY

100

GiB

☐

Enable ListBucket access for all users on the storage VM "svm_demo".
Enabling this will allow users to access the bucket.

More options

Cancel

Save

Nella sezione "altre opzioni" selezionare la casella di controllo attiva versione e fare clic sul pulsante "Salva".

Add bucket

NAME

bucket

FOLDER (OPTIONAL)

Browse

Specify the folder to map to this bucket. [Know more](#)

CAPACITY

100

GiB

☐ Use for tiering

If you select this option, the system will try to select low-cost media with optimal performance for the tiered data.

☒ Enable versioning

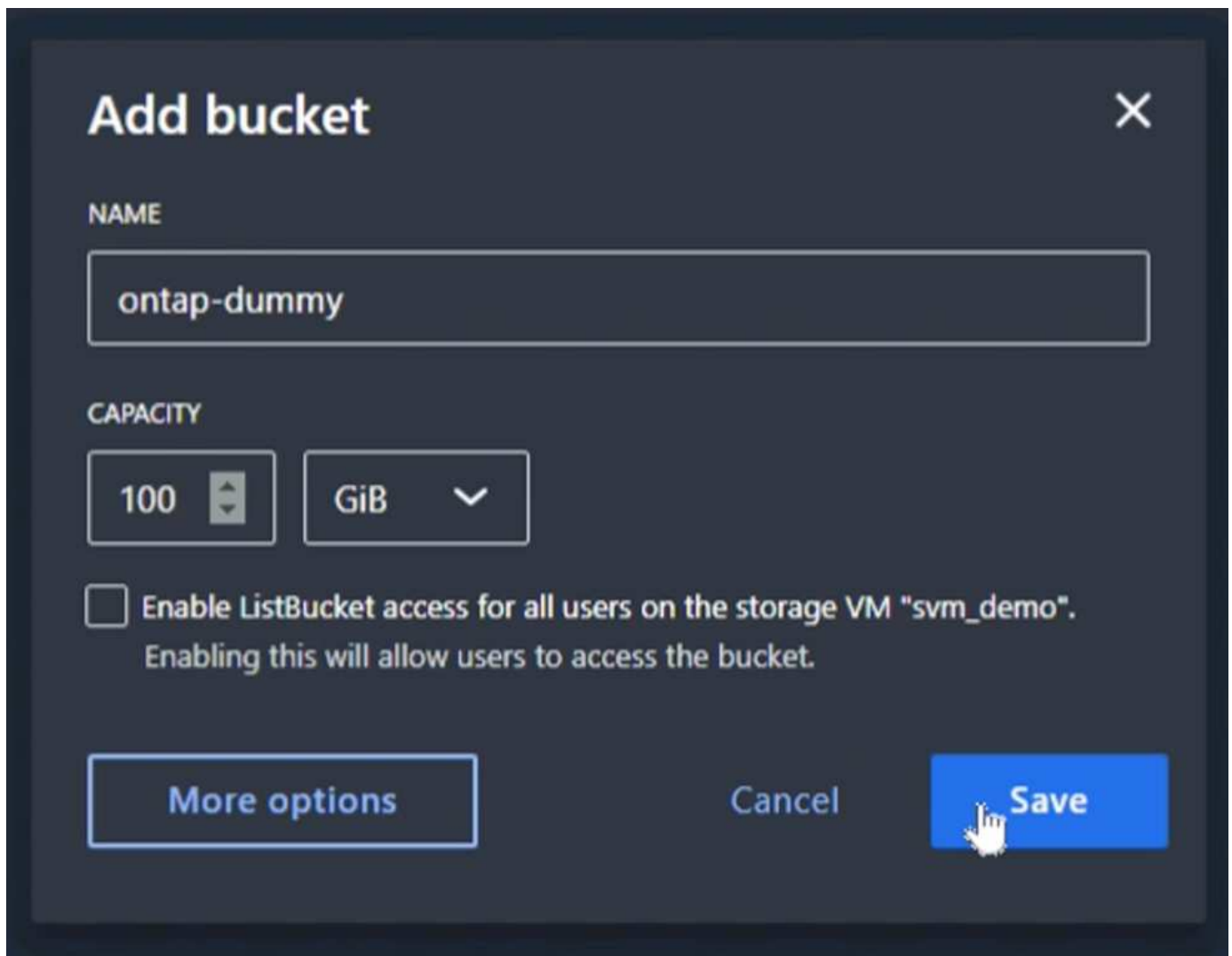
Versioning-enabled buckets allow you to recover objects that were accidentally deleted or overwritten. After versioning is enabled, it can't be disabled. However, you can suspend versioning.

PERFORMANCE SERVICE LEVEL

Extreme

Not sure? [Get help selecting type](#)

Ripetere il processo e creare un secondo bucket senza attivare il controllo delle versioni. Immettere un nome con la stessa capacità del bucket uno e deselezionare la casella di controllo "Abilita accesso a ListBucket...", quindi fare clic sul pulsante "Salva".



Add bucket ✕

NAME

ontap-dummy

CAPACITY

100 ▲ ▼ GiB ▼

☐ Enable ListBucket access for all users on the storage VM "svm_demo".
Enabling this will allow users to access the bucket.

More options Cancel Save

Di Rafael Guedes e Aron Klein

Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID

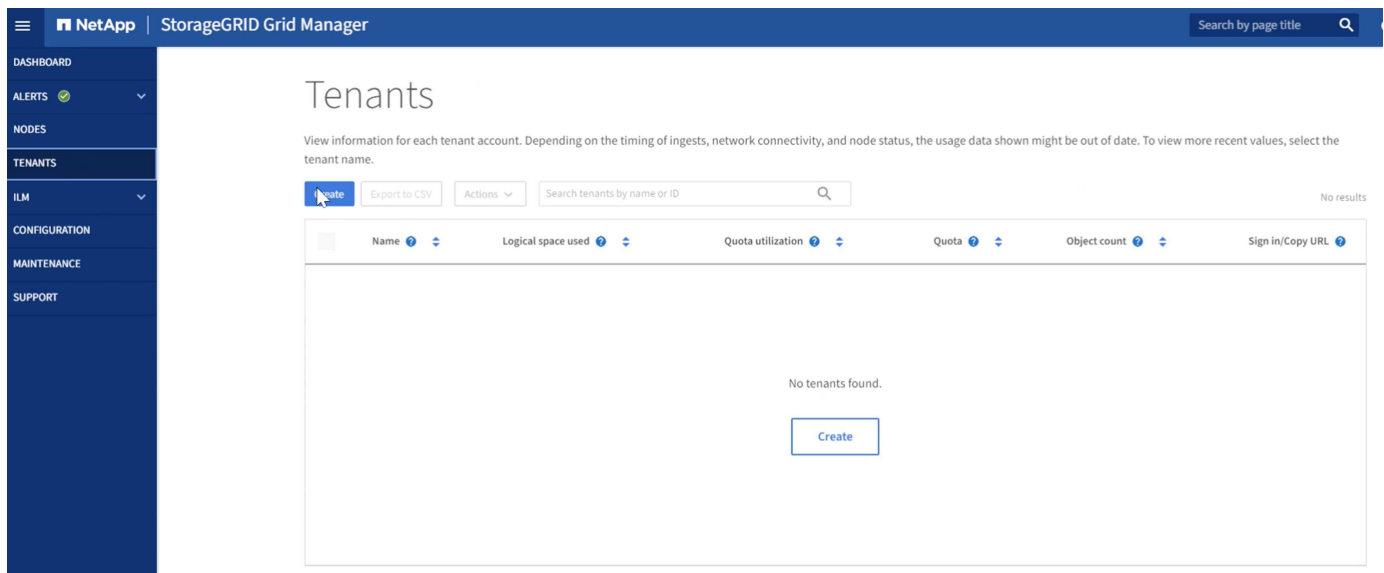
Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID

Preparazione di StorageGRID

Continuando la configurazione per questa demo, creeremo un tenant, un utente, un gruppo di sicurezza, una policy di gruppo e un bucket.

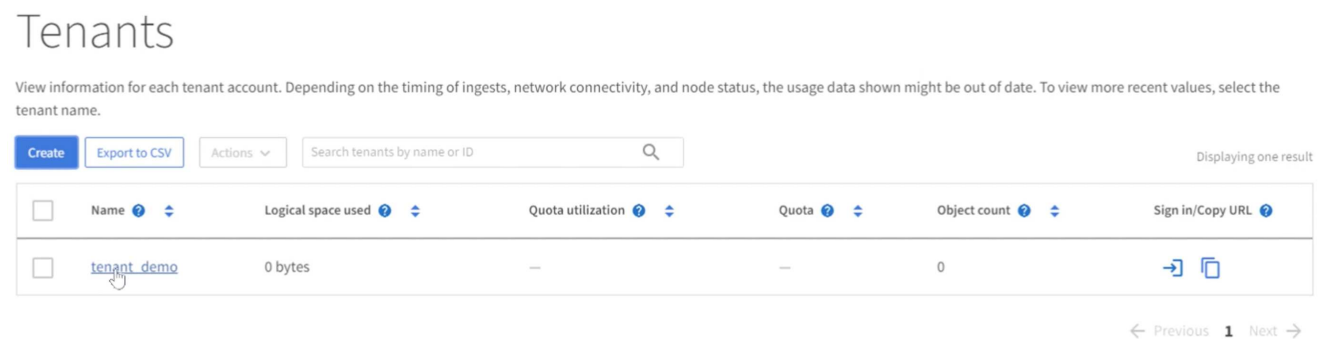
Creare il tenant

Passare alla scheda "inquilini" e fare clic sul pulsante "Crea"



Inserire i dettagli del tenant che fornisce il nome del tenant, selezionare S3 per il tipo di client e non è richiesta alcuna quota. Non è necessario selezionare i servizi della piattaforma o consentire la selezione S3. Se lo si sceglie, è possibile scegliere di utilizzare la propria fonte di identità. Impostare la password principale e fare clic sul pulsante Finish (fine).

Fare clic sul nome del tenant per visualizzare i dettagli del tenant. **In seguito sarà necessario l'ID tenant, quindi copiarlo.** Fare clic sul pulsante Accedi. In questo modo si accede al portale tenant. Salvare l'URL per uso futuro.




In questo modo si accede al portale tenant. Salvare l'URL per uso futuro e immettere le credenziali dell'utente root.

← → ↻ ⚠ Not secure | 192.168.0.80/?accountId=27041610751165610501

🔍 Lab Status 🔍 Power Controls 🔍 Accounts 🔍 cluster1-mgmt 🔍 cluster2-mgmt 🔍 Blue XP

NetApp Support | NetApp



StorageGRID® Tenant Manager

Recent -- Optional -- ▾

Account ID 27041610751165610501

Username root

Password ••••••

Sign in

Creare l'utente

Accedere alla scheda utenti e creare un nuovo utente.

☰

NetApp | StorageGRID Tenant Manager

DASHBOARD

STORAGE (S3) ^

My access keys

Buckets

Platform services endpoints

ACCESS MANAGEMENT ^

Groups

Users

Identity federation

Users

View local and federated users. Edit properties and group membership of local users.

1 user [Create user](#)

Actions ▾

<input type="checkbox"/>	Username ↕	Full Name ↕	Denied ↕	Type ↕
<input type="checkbox"/>	root	Root		Local

← Previous 1 Next →

Optional

Enter user credentials

Create a new local user and configure user access.

Full name ?

Must contain at least 1 and no more than 128 characters

Username ?

Password

Must contain at least 8 and no more than 32 characters

Confirm password

Deny access

Do you want to prevent this user from signing in regardless of assigned group permissions?

☐ Yes ☒ No

[Cancel](#) [Continue](#)

Ora che il nuovo utente è stato creato, fare clic sul nome dell'utente per aprire i dettagli dell'utente.

Copiare l'ID utente dall'URL da utilizzare in un secondo momento.

Not secure | https://192.168.0.80/ui/#/users/ebc132e2-cfc3-42c0-a445-3b4465cb523c

Power Controls Accounts cluster1-mgmt cluster2-mgmt Blue XP

NetApp | StorageGRID Tenant Manager

Users > Demo S3 User

Overview

Full name: ?	Demo S3 User
Username: ?	demo_s3_user
User type: ?	Local
Denied access: ?	Yes
Access mode: ?	No Groups
Group membership: ?	None

[Password](#)
[Access](#)
[Access keys](#)
[Groups](#)

Change password

Change this user's password.

Per creare i tasti S3, fare clic sul nome utente.

NetApp | StorageGRID Tenant Manager

Users

View local and federated users. Edit properties and group membership of local users.

2 users

Actions ▾

<input type="checkbox"/>	Username ▾	Full Name ▾	Denied ▾	Type ▾
<input type="checkbox"/>	root	Root		Local
<input type="checkbox"/>	demo_s3_user	Demo S3 User	✓	Local

← Previous 1 Next →

Selezionare la scheda "tasti di accesso" e fare clic sul pulsante "Crea chiave". Non è necessario impostare un'ora di scadenza. Scaricare i S3 tasti in quanto non possono essere richiamati una volta chiusa la finestra.

Create access key



Choose expiration time

2

Download access key

Download access key

To save the keys for future reference, select **Download .csv**, or copy and paste the values to another location.



You will not be able to view the Access key ID or Secret access key after you close this dialog.

Access key ID

7CT7L1X5MIO5091E86TR



Secret access key

RIJnC5N5FX9RSWgFdj6SQ7wMrfRZYu5bQLdNQTOc



Download .csv

Finish

Creare il gruppo di protezione

Andare alla pagina gruppi e creare un nuovo gruppo.

Create group

1 Choose a group type

2 Manage permissions

3 Set S3 group policy

4 Add users
Optional

Choose a group type ?

Create a new local group or import a group from the external identity source.

Local group

Federated group

Create local groups to assign permissions to any local users you defined in StorageGRID.

Display name

Demo S3 Group

Must contain at least 1 and no more than 32 characters

Unique name ?

demo_s3_group

Cancel

Continue

Impostare le autorizzazioni del gruppo su sola lettura. Si tratta delle autorizzazioni dell'interfaccia utente tenant, non delle autorizzazioni S3.

✓ Choose a group type

2 Manage permissions

3 Set S3 group policy

4 Add users
Optional

Manage group permissions

Select an access mode for this group and select one or more permissions.

Access mode ?

Select whether users can change settings and perform operations or whether they can only view settings and features.

☐ Read-write ☒ Read-only

Group permissions ?

Select the permissions you want to assign to this group.

☐ **Root access**
Allows users to access all administration features. Root access permission supersedes all other permissions.

☐ **Manage all buckets**
Allows users to change settings of all S3 buckets (or Swift containers) in this account.

☐ **Manage endpoints**
Allows users to configure endpoints for platform services.

☐ **Manage your own S3 credentials**
Allows users to create and delete their own S3 access keys.

[Previous](#) [Continue](#)

Le autorizzazioni S3 sono controllate con i criteri di gruppo (criteri IAM). Impostare il criterio di gruppo su personalizzato e incollare il criterio json nella casella. Questo criterio consente agli utenti di questo gruppo di elencare i bucket del tenant ed eseguire qualsiasi operazione S3 nel bucket denominato "bucket" o sottocartelle nel bucket denominato "bucket".

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:ListAllMyBuckets",
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": ["arn:aws:s3:::bucket", "arn:aws:s3:::bucket/*"]
    }
  ]
}
```

×

Create group

✓ Choose a group type

✓ Manage permissions

3 Set S3 group policy

4 Add users
Optional

Set S3 group policy ?

An S3 group policy controls user access permissions to specific S3 resources, including buckets. Non-root users have no access by default.

☐ No S3 Access
 ☐ Read Only Access
 ☐ Full Access
 ☒ Custom
 (Must be a valid JSON formatted string.)

```
{
  "Effect": "Allow",
  "Action": "s3:ListAllMyBuckets",
  "Resource": "arn:aws:s3:::"
},
{
  "Effect": "Allow",
  "Action": "s3:*",
  "Resource": ["arn:aws:s3:::bucket", "arn:aws:s3:::bucket/*"]
}
]
```

Previous

Continue

Infine, aggiungere l'utente al gruppo e terminare.

Create group

✓ Choose a group type

✓ Manage permissions

✓ Set S3 group policy

4 Add users
Optional

Add users

(This step is optional. If required, you can save this group and add users later.)

Select local users to add to the group **Demo S3 Group**.

<input checked="" type="checkbox"/>	Username	Full Name	Denied
<input checked="" type="checkbox"/>	demo_s3_user	Demo S3 User	<input checked="" type="checkbox"/>

[Previous](#)

Create group

Creare due bucket

Passare alla scheda bucket e fare clic sul pulsante Crea bucket.

NetApp | StorageGRID Tenant Manager

DASHBOARD

STORAGE (S3)

My access keys

Buckets

Platform services endpoints

ACCESS MANAGEMENT

Groups

Users

Identity federation

Buckets

Create buckets and manage bucket settings.

0 buckets

Create bucket

Experimental S3 Console

Actions

	Name	Region	Object Count	Space Used	Date Created
No buckets found					

Create bucket

Definire il nome del bucket e la regione.

Create bucket

1

Enter details

2

Manage object settings
Optional

Enter bucket details

Enter the bucket's name and select the bucket's region.

Bucket name ?

bucket

Region ?

us-east-1

Cancel

Continue

In questo primo bucket abilitare la versione.

Create bucket

✓

Enter details

2

Manage object settings
Optional

Manage object settings

Optional

Object versioning

Enable object versioning if you want to store every version of each object in this bucket. You can then retrieve previous versions of an object as needed.

✓

Enable object versioning

Previous

Create bucket

Ora creare un secondo bucket senza abilitare il controllo delle versioni.

Create bucket

1

Enter details

2

Manage object settings
Optional

Enter bucket details

Enter the bucket's name and select the bucket's region.

Bucket name ?

sg-dummy

Region ?

us-east-1

CancelContinue

Non abilitare la versione in questo secondo bucket.

Create bucket

✓

Enter details

2

Manage object settings
Optional

Manage object settings Optional

Object versioning

Enable object versioning if you want to store every version of each object in this bucket. You can then retrieve previous versions of an object as needed.

☐ Enable object versioning

PreviousCreate bucket

Di Rafael Guedes e Aron Klein


Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID


Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID

Compilare il bucket Source (origine)

Consente di inserire alcuni oggetti nel bucket ONTAP di origine. Utilizzeremo S3Browser per questa demo, ma puoi usare qualsiasi strumento che ti trovi a tuo agio.

Utilizzando le chiavi S3 dell'utente ONTAP create in precedenza, configurare S3Browser per la connessione al sistema ONTAP.

 Add New Account



Add New Account

Enter new account details and click Add new account

[online help](#)

Display name:

Bucket (original and post-migration)

Assign any name to your account.

Account type:

S3 Compatible Storage

Choose the storage you want to work with. Default is Amazon S3 Storage.

REST Endpoint:

s3portal.demo.netapp.com:8080

Specify S3-compatible API endpoint. It can be found in storage documentation. Example: rest.server.com:8080

Access Key ID:

3TVPI142JGE3Y7FV2KC0

Required to sign the requests you send to Amazon S3, see more details at <https://s3browser.com/keys>

Secret Access Key:

.....

Required to sign the requests you send to Amazon S3, see more details at <https://s3browser.com/keys>


☐ Encrypt Access Keys with a password:


Turn this option on if you want to protect your Access Keys with a master password.

☐ Use secure transfer (SSL/TLS)

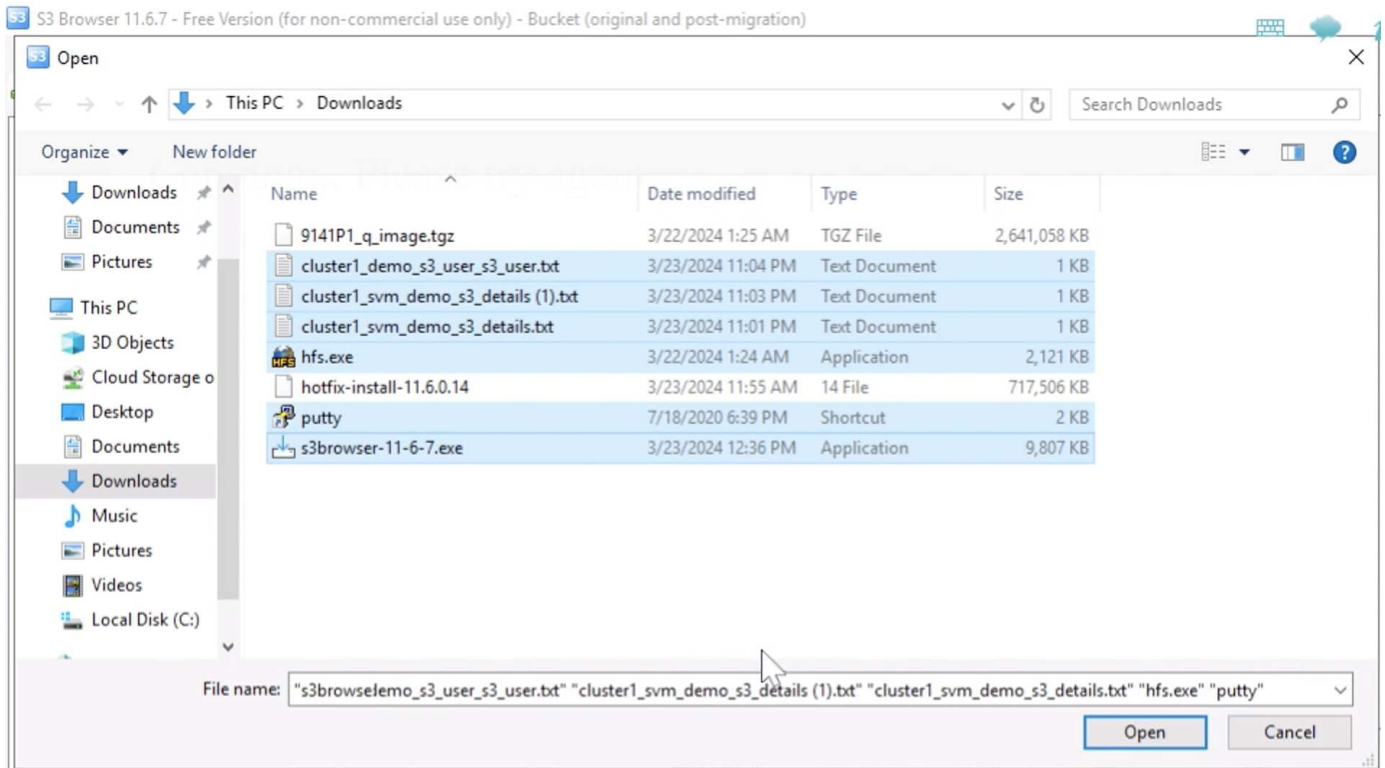
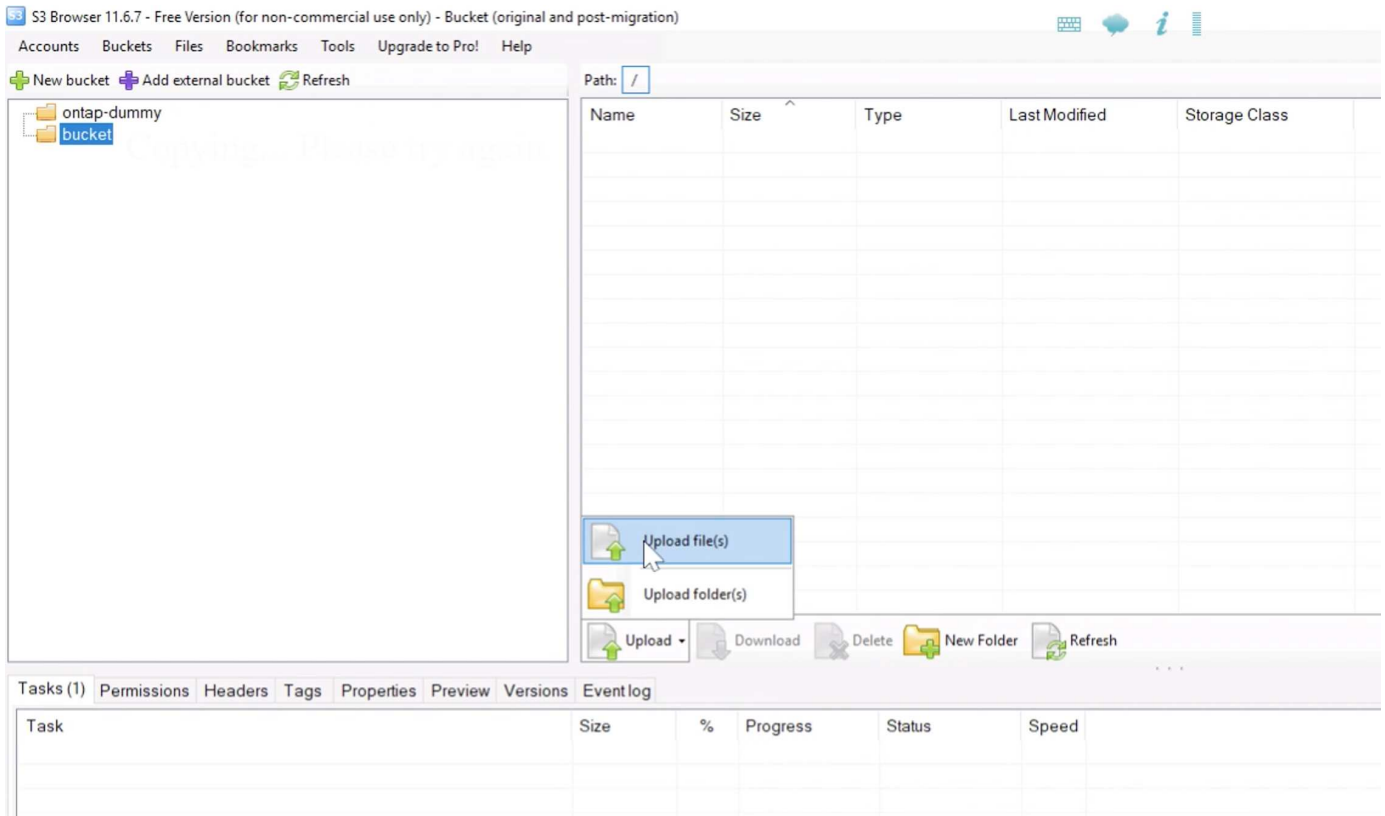
If checked, all communications with the storage will go through encrypted SSL/TLS channel

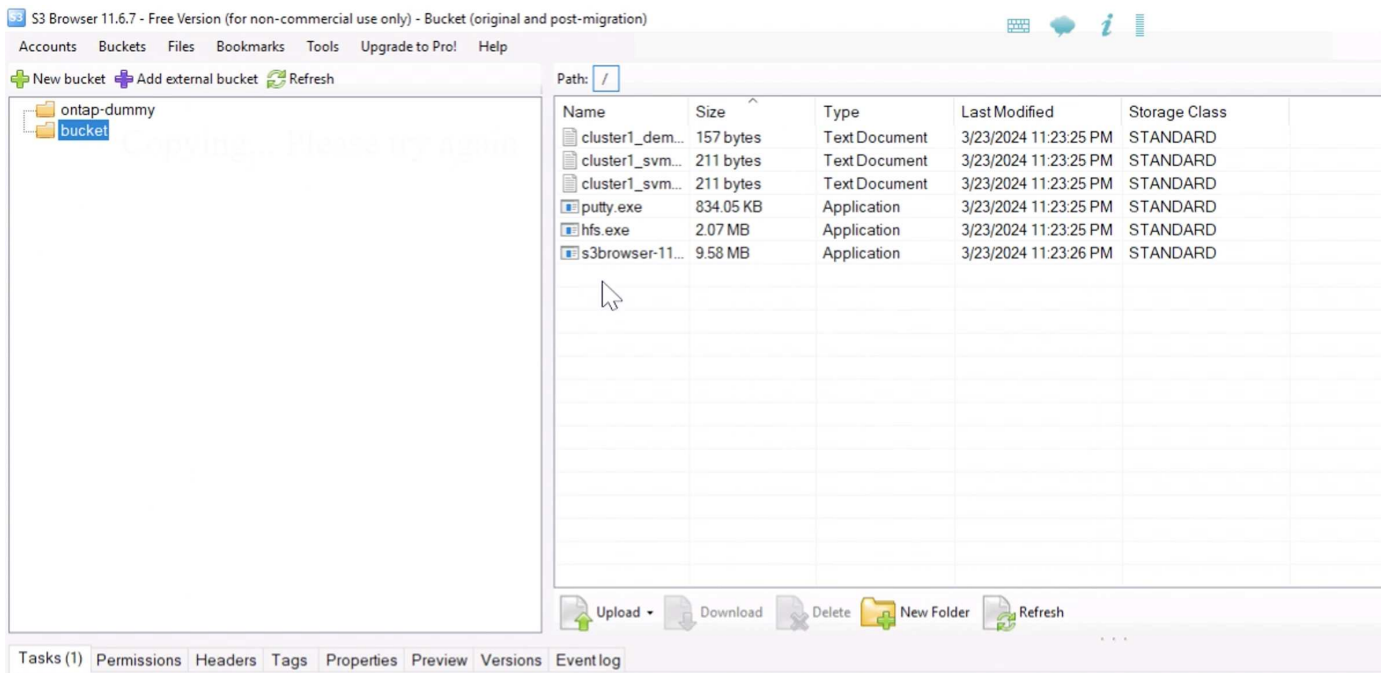
[advanced settings..](#)

 Add new account

 Cancel

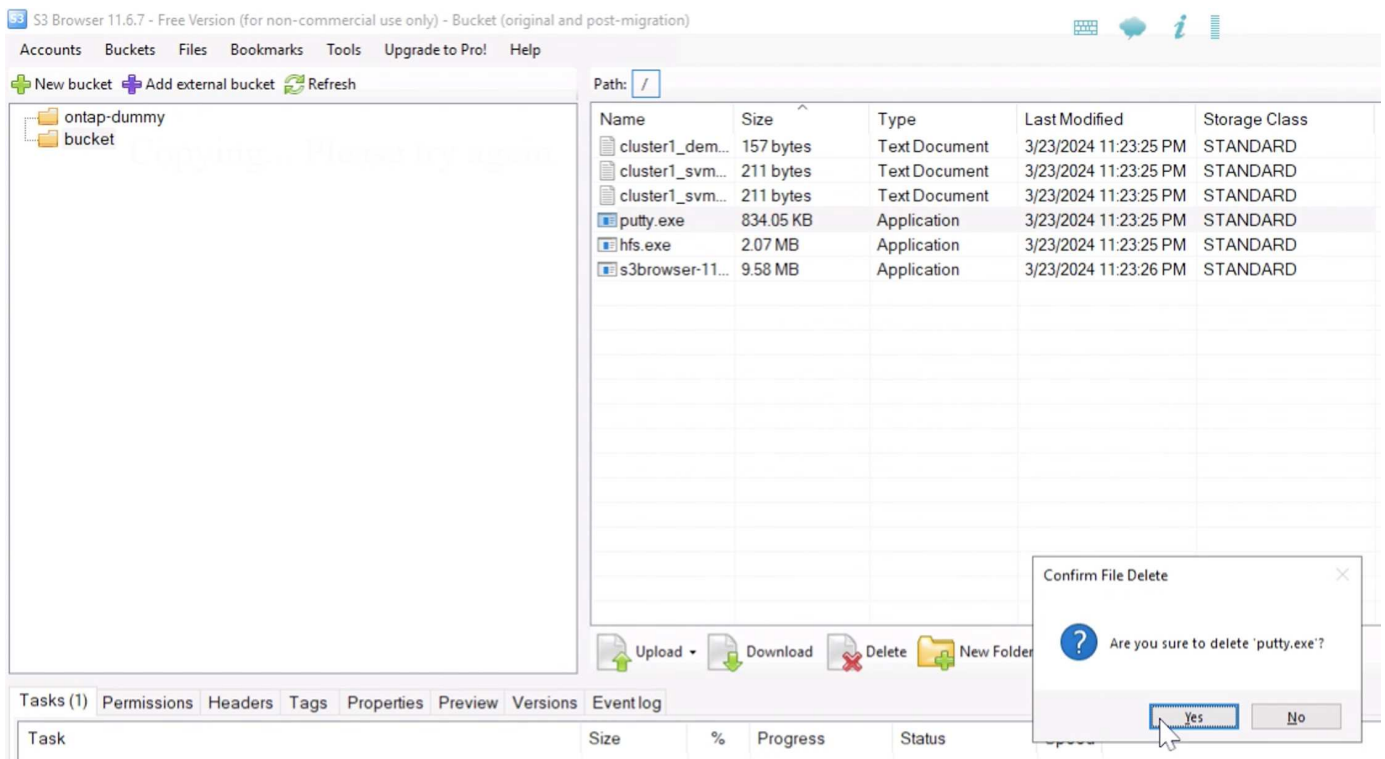
Ora permette di caricare alcuni file nel bucket abilitato per la versione.



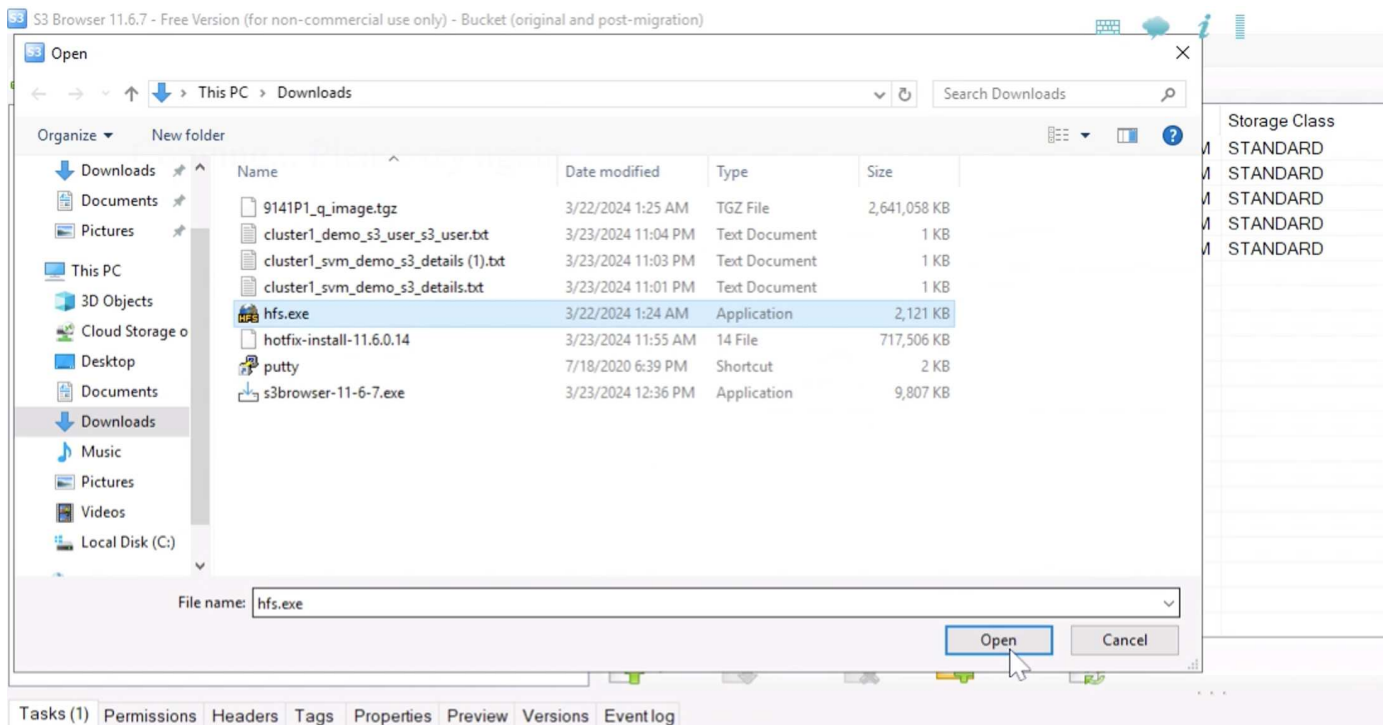


Ora permette di creare alcune versioni di oggetti nel bucket.

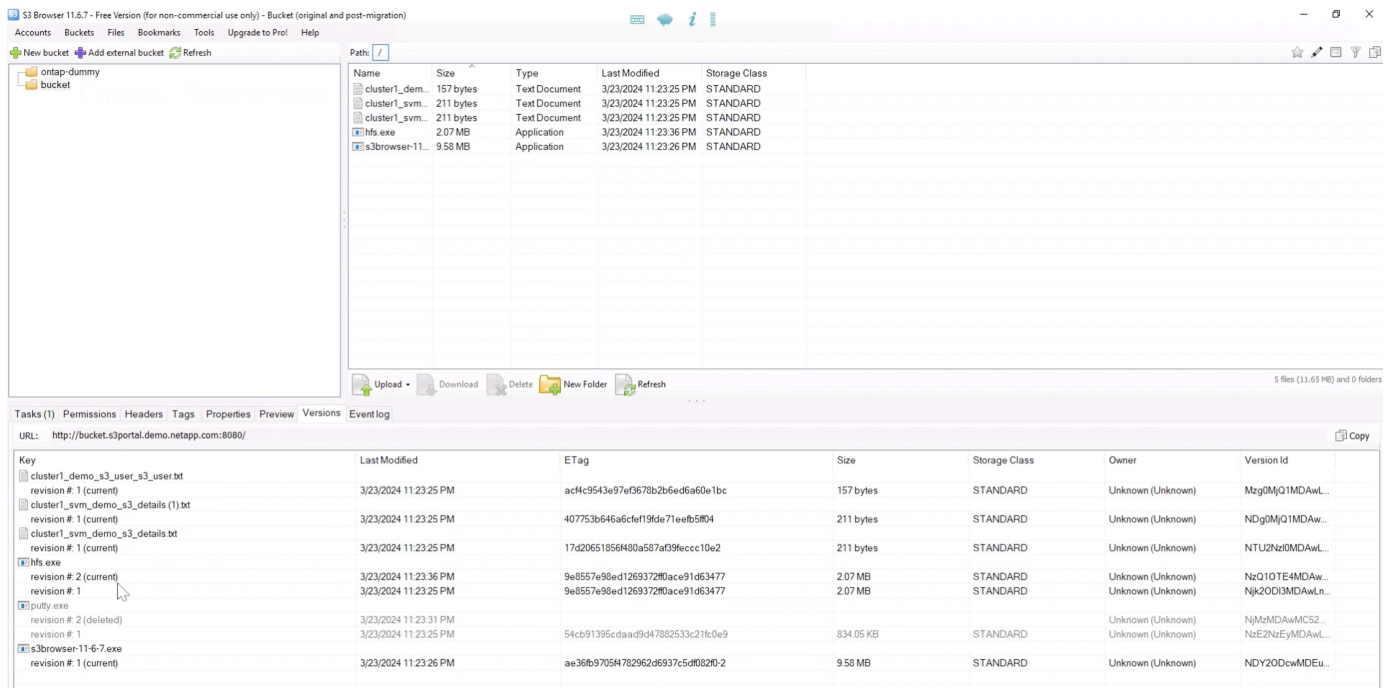
Eliminare un file.



Caricare un file già esistente nel bucket per copiare il file su se stesso e crearne una nuova versione.



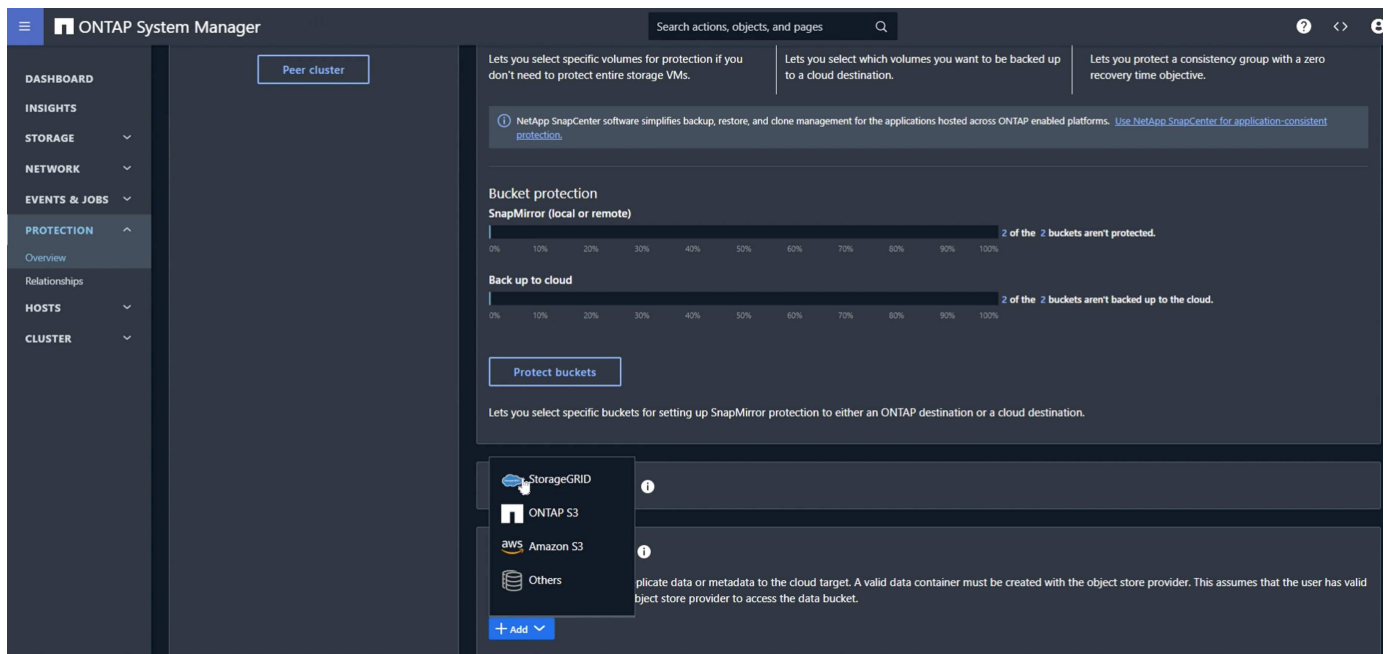
In S3Browser possiamo visualizzare le versioni degli oggetti appena creati.



Stabilire la relazione di replica

Consente di iniziare a inviare dati da ONTAP a StorageGRID.

In Gestione di sistema di ONTAP, selezionare "protezione/Panoramica". Scorri verso il basso fino a "Archivio oggetti cloud", quindi fai clic sul pulsante "Aggiungi" e seleziona "StorageGRID".



Inserisci le informazioni StorageGRID fornendo un nome, uno stile URL (per questa demo useremo gli URL Path-style). Impostare l'ambito dell'archivio oggetti su "Storage VM".

Add cloud object store

NAME

sgws_demo

URL STYLE

Path-style URL

OBJECT STORE SCOPE

☐ Cluster ☒ Storage VM

USE BY

☐ SnapMirror ☒ ONTAP S3 SnapMirror

SERVER NAME (FQDN)

192.168.0.80

Se si utilizza SSL, impostare la porta dell'endpoint del bilanciamento del carico e copiarla nel certificato

dell'endpoint StorageGRID. Altrimenti deselezionare la casella SSL e immettere la porta dell'endpoint HTTP qui.

Immettere i tasti S3 dell'utente StorageGRID e il nome del bucket dalla configurazione StorageGRID riportata sopra per la destinazione.

The screenshot shows a configuration window for a cloud object store. It has three input fields at the top: 'ACCESS KEY' with the value '7CT7L1X5MIO5091E86TR', 'SECRET KEY' with masked dots, and 'CONTAINER NAME' with the value 'bucket'. Below these is a section titled 'Network for cloud object store' which contains a table with network details and a 'Considerations' link.

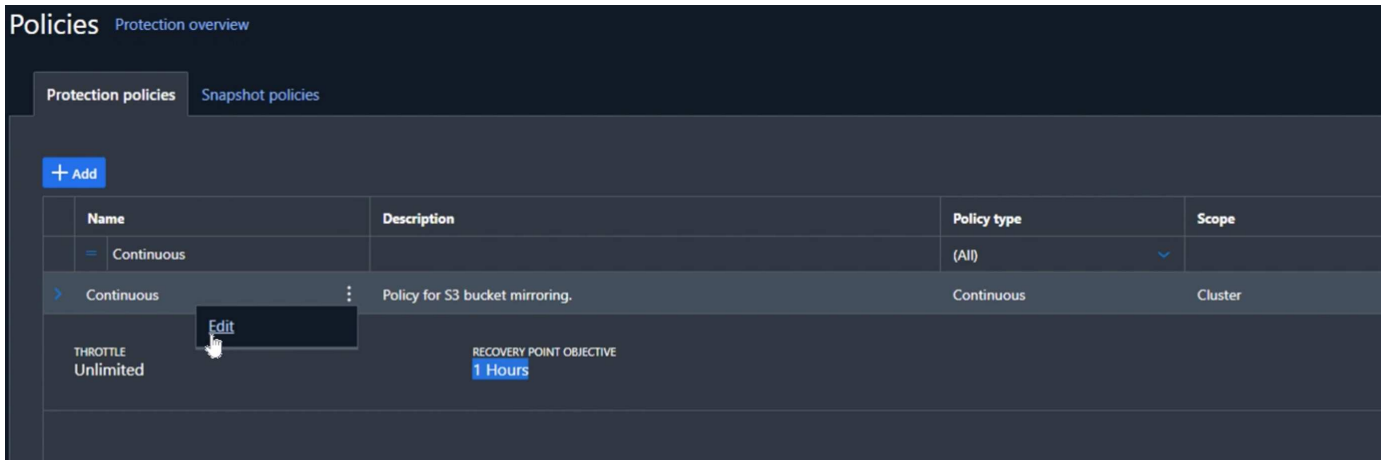
NODE	IP ADDRESS	SUBNET MASK	BROADCAST DOMAIN	GATEWAY
onPrem-01	192.168.0.113	24	Default	192.168.0.1

Below the table is a checkbox 'Use HTTP proxy' which is unchecked. At the bottom are 'Save' and 'Cancel' buttons.

Una volta configurata una destinazione, è possibile configurare le impostazioni dei criteri per la destinazione. Espandere "Impostazioni criteri locali" e selezionare "continuo".

The screenshot shows the ONTAP System Manager web interface. The left sidebar has a menu with 'PROTECTION' selected. The main content area shows 'Back up to cloud' progress and 'Local policy settings'. Under 'Local policy settings', there are three panels: 'Protection policies', 'Snapshot policies', and 'Schedules'. In the 'Schedules' panel, the 'Continuous' option is selected, and the '5min' schedule is highlighted.

Modificare il criterio continuo e modificare l'obiettivo del punto di ripristino da "1 ore" a "3 secondi".



Ora possiamo configurare SnapMirror per replicare il bucket.

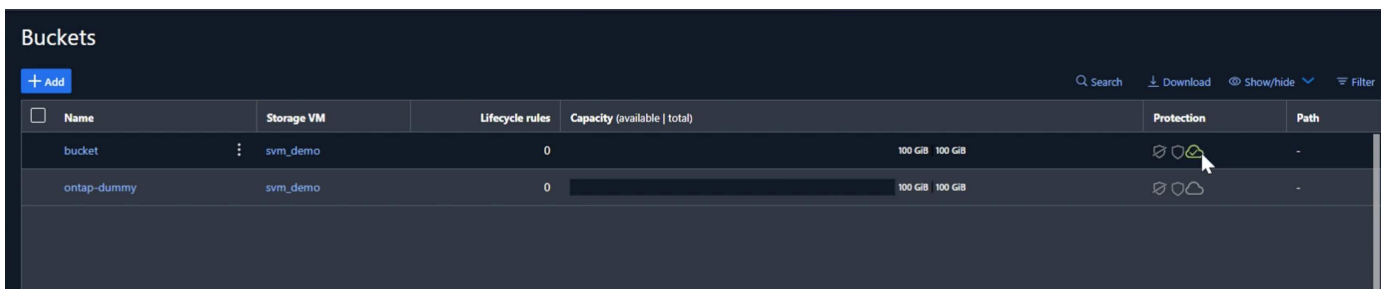
SnapMirror create -source-path sv_demo: /Bucket/bucket -destination-path sgws_demo: /Objstore -policy Continuous

```
cluster1-mgmt
Using username "admin".
Using keyboard-interactive authentication.
Password:

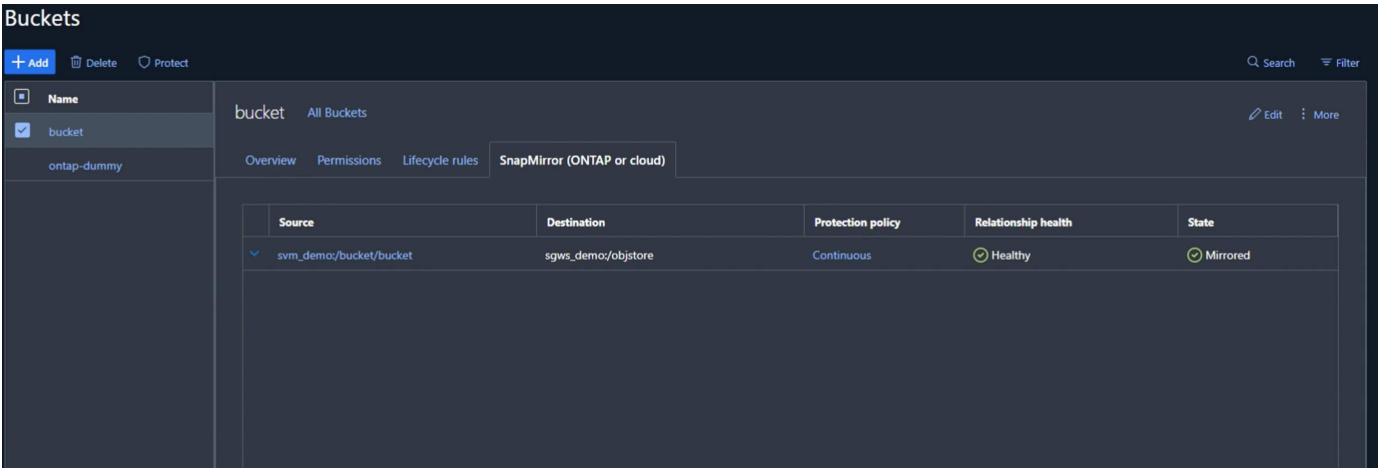
Last login time: 3/24/2024 00:02:00
cluster1::> snapmirror create -source-path sv_demo:/bucket/bucket -destination-path sgws_demo:/objstore -policy Continuous
[Job 220] Job is queued: Create an S3 SnapMirror relationship between bucket "sv_demo:bucket" and bucket "objstore/sgws_demo"..

cluster1::> █
```

Il bucket mostrerà ora un simbolo di nuvola nell'elenco bucket sotto protezione.

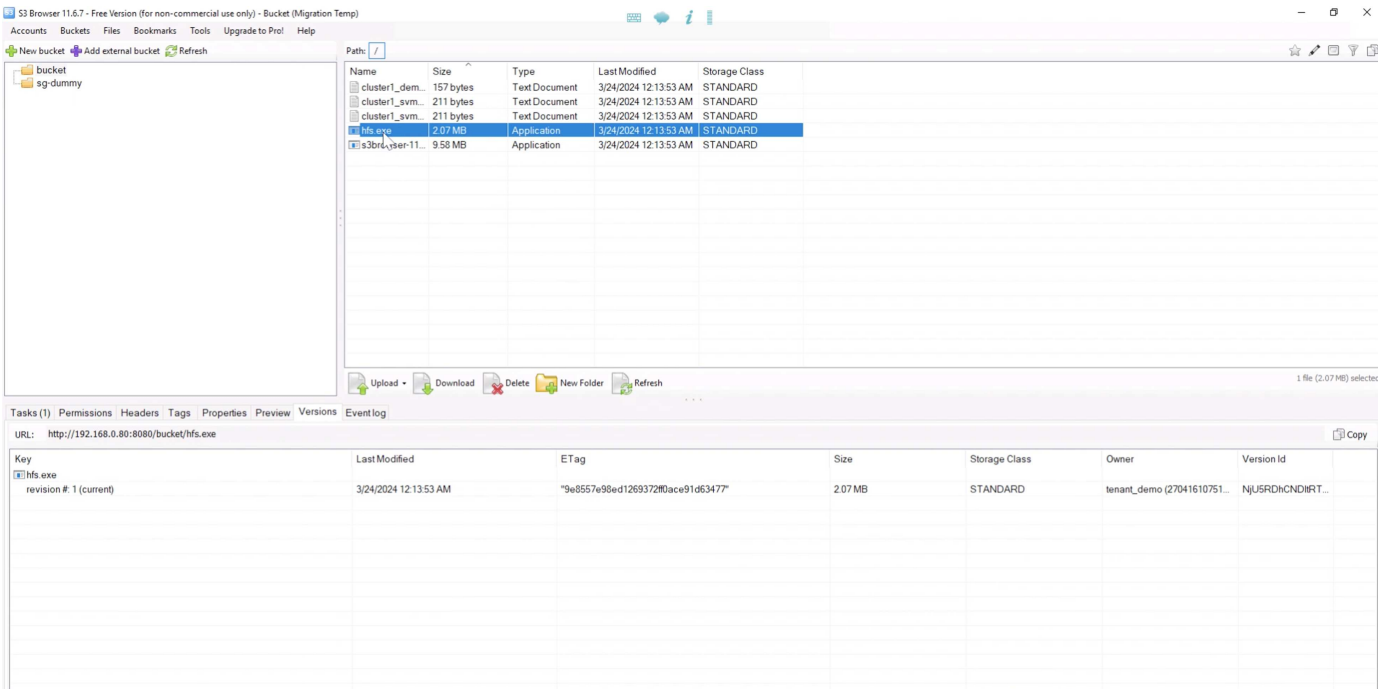


Se si seleziona il bucket e si passa alla scheda "SnapMirror (ONTAP o Cloud)", verrà visualizzato lo stato di spedizione SnapMirror.



I dettagli della replica

Ora disponiamo di un bucket di replica con successo da ONTAP a StorageGRID. Ma che cosa si replica? La nostra fonte e la nostra destinazione sono entrambi bucket in versione. Anche le versioni precedenti vengono replicate nella destinazione? Se guardiamo al nostro bucket StorageGRID con S3Browser vediamo che le versioni esistenti non sono state replicate e l'oggetto eliminato non esiste, né un marcatore di eliminazione per quell'oggetto. L'oggetto duplicato ha solo la versione 1 nel bucket StorageGRID.



Nel bucket ONTAP, si aggiunge una nuova versione allo stesso oggetto utilizzato in precedenza e si osserva come viene replicata.

S3 Browser 11.6.7 - Free Version (for non-commercial use only) - Bucket (original and post-migration)

Accounts Buckets Files Bookmarks Tools Upgrade to Pro! Help

New bucket Add external bucket Refresh

Path: /

Name	Size	Type	Last Modified	Storage Class
cluster1_demo...	157 bytes	Text Document	3/23/2024 11:23:25 PM	STANDARD
cluster1_svm...	211 bytes	Text Document	3/23/2024 11:23:25 PM	STANDARD
cluster1_svm...	211 bytes	Text Document	3/23/2024 11:23:25 PM	STANDARD
putty.exe	834.05 KB	Application	3/23/2024 11:23:25 PM	STANDARD
hfs.exe	2.07 MB	Application	3/24/2024 12:14:52 AM	STANDARD
s3browser-11...	9.58 MB	Application	3/23/2024 11:23:26 PM	STANDARD

6 files (12.46 MB) and 0 folders

Tasks (1) Permissions Headers Tags Properties Preview Versions Event log

URL: http://bucket.s3portal.demo.netapp.com:8080/

Key	Last Modified	ETag	Size	Storage Class	Owner	Version Id
cluster1_demo_s3_user_s3_user.txt						
revision # 1 (current)	3/23/2024 11:23:25 PM	ac4c9543e97ef0678b2b6e6a60e1bc	157 bytes	STANDARD	Unknown (Unknown)	Mzg0MjQ1MDAw...
cluster1_svm_demo_s3_details (1).txt	3/23/2024 11:23:25 PM	407753b646a6cfe1f9de71eebf5f04	211 bytes	STANDARD	Unknown (Unknown)	NDg0MjQ1MDAw...
revision # 1 (current)	3/23/2024 11:23:25 PM	17d20651856480a587af39fccc10e2	211 bytes	STANDARD	Unknown (Unknown)	NTU2Nz00MDAw...
hfs.exe						
revision # 3 (current)	3/24/2024 12:14:52 AM	9e8557e98ed1269372f0ace91d63477	2.07 MB	STANDARD	Unknown (Unknown)	NTY0NDg0MDAw...
revision # 2	3/23/2024 11:23:36 PM	9e8557e98ed1269372f0ace91d63477	2.07 MB	STANDARD	Unknown (Unknown)	NzQ1OTI0MDAw...
revision # 1	3/23/2024 11:23:25 PM	9e8557e98ed1269372f0ace91d63477	2.07 MB	STANDARD	Unknown (Unknown)	Njk2ODI0MDAw...
putty.exe						
revision # 1 (current)	3/23/2024 11:23:25 PM	54cb91395cdaad94788253c21fc0e9	834.05 KB	STANDARD	Unknown (Unknown)	NzE2NzE0MDAw...
s3browser-11-6-7.exe						
revision # 1 (current)	3/23/2024 11:23:26 PM	ae36be97054782962d6937c5d0820-2	9.58 MB	STANDARD	Unknown (Unknown)	NDY2ODcwMDEu...

Se guardiamo al lato StorageGRID vediamo che è stata creata anche una nuova versione in questo bucket, ma manca la versione iniziale da prima della relazione SnapMirror.

S3 Browser 11.6.7 - Free Version (for non-commercial use only) - Bucket (Migration Temp)

Accounts Buckets Files Bookmarks Tools Upgrade to Pro! Help

New bucket Add external bucket Refresh

Path: /

Name	Size	Type	Last Modified	Storage Class
cluster1_demo...	157 bytes	Text Document	3/24/2024 12:13:53 AM	STANDARD
cluster1_svm...	211 bytes	Text Document	3/24/2024 12:13:53 AM	STANDARD
cluster1_svm...	211 bytes	Text Document	3/24/2024 12:13:53 AM	STANDARD
putty.exe	834.05 KB	Application	3/24/2024 12:14:28 AM	STANDARD
hfs.exe	2.07 MB	Application	3/24/2024 12:14:56 AM	STANDARD
s3browser-11...	9.58 MB	Application	3/24/2024 12:13:53 AM	STANDARD

1 file (2.07 MB)

Tasks (1) Permissions Headers Tags Properties Preview Versions Event log

URL: http://192.168.0.80:8080/bucket/hfs.exe

Key	Last Modified	ETag	Size	Storage Class	Owner	Version Id
hfs.exe						
revision # 2 (current)	3/24/2024 12:14:56 AM	"9e8557e98ed1269372f0ace91d63477"	2.07 MB	STANDARD	tenant_demo (27041610751...	OEHRyY4NDgRT...
revision # 1	3/24/2024 12:13:53 AM	"9e8557e98ed1269372f0ace91d63477"	2.07 MB	STANDARD	tenant_demo (27041610751...	NjU5RDh0NDIIR...

Questo perché il processo di ONTAP SnapMirror S3 replica solo la versione corrente dell'oggetto. Ecco perché abbiamo creato un bucket di versione sul lato StorageGRID per essere la destinazione. In questo modo StorageGRID può mantenere una cronologia delle versioni degli oggetti.

Di Rafael Guedes e Aron Klein

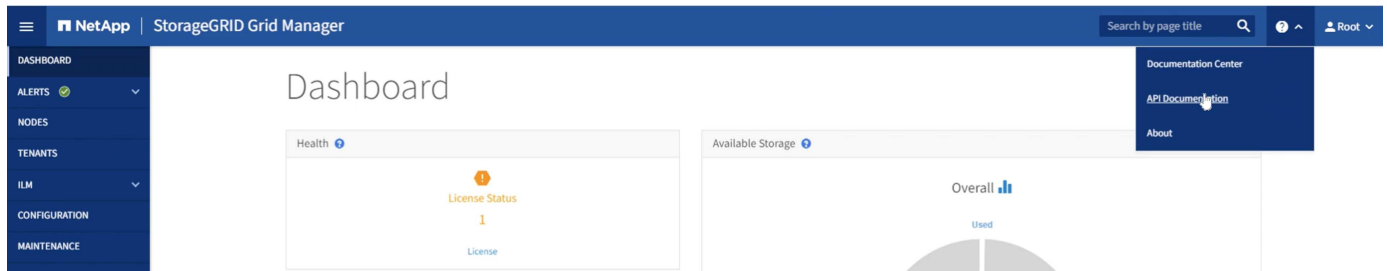
Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID

Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID

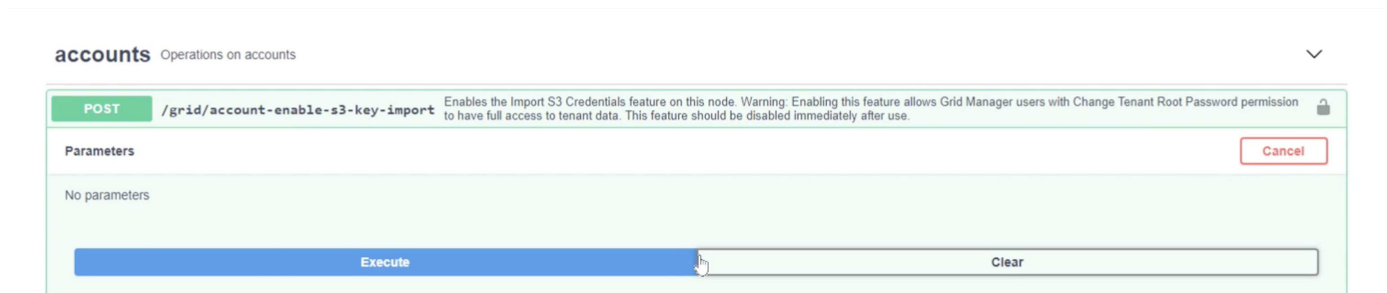
Migrare S3 chiavi

Per una migrazione, la maggior parte del tempo si desidera migrare le credenziali per gli utenti invece di generare nuove credenziali sul lato di destinazione. StorageGRID fornisce api per consentire l'importazione di S3 chiavi per un utente.

Accedendo all'interfaccia utente di gestione di StorageGRID (non all'interfaccia utente di gestione tenant), aprire la pagina dello swap della documentazione API.



Espandere la sezione "account", selezionare "POST /grid/account-enable-S3-key-import", fare clic sul pulsante "prova", quindi fare clic sul pulsante "Esegui".



Ora scorri verso il basso ancora sotto "Accounts" fino a "POST /grid/accounts/{id}/users/{user_id}/S3-access-keys"

Qui è dove stiamo andando inserire l'ID del inquilino e l'ID dell'account utente che abbiamo raccolto in precedenza. Compilare i campi e le chiavi del nostro utente ONTAP nella casella json. È possibile impostare la scadenza delle chiavi, o rimuovere il " , "expires": 123456789" e fare clic su execute.

POST
/grid/accounts/{id}/users/{user_id}/s3-access-keys
Imports S3 credentials for a given user in a tenant account

Parameters

Name	Description
id * required string (path)	ID of Storage Tenant Account <input type="text" value="27041610751165610501"/>
user_id * required string (path)	ID of user in tenant account. <input type="text" value="ebc132e2-cfc3-42c0-a445-3b4465cb523c"/>
body * required (body)	<div>Edit Value Model</div> <pre>{ "accessKey": "3TVPI142JGE3Y7FV2KC0", "secretAccessKey": "75a1QqKBU4quA132twI4g41C4Gg5PP30ncy0sPE8" }</pre>

Una volta completate tutte le importazioni della chiave utente, disabilitare la funzione di importazione della chiave in "account" "POST /grid/account-disable-s3-key-import"

POST
/grid/account-disable-s3-key-import
Disables the Import S3 Credentials feature on this node.

Parameters

No parameters

Execute


Responses

Response content type application/json

Cancel

Se guardiamo l'account utente nell'interfaccia utente del gestore tenant, possiamo vedere che è stata aggiunta la nuova chiave.

Overview


Full name: ?	Demo S3 User 
Username: ?	demo_s3_user
User type: ?	Local
Denied access: ?	Yes
Access mode: ?	Read-only
Group membership: ?	Demo S3 Group



[Password](#)[Access](#)[Access keys](#)[Groups](#)

Manage access keys

Add or delete access keys for this user.

[Create key](#)

Actions 

<input type="checkbox"/>	Access key ID 	Expiration time 
<input type="checkbox"/>	*****86TR	None
<input type="checkbox"/>	*****2KC0	None

Il taglio finale

Se l'intenzione è quella di avere un bucket a replica perpetua da ONTAP a StorageGRID, puoi finire qui. Se si tratta di una migrazione da ONTAP S3 a StorageGRID, allora è il momento di mettersi fine e tagliare.

In Gestione di sistema di ONTAP, modificare il gruppo S3 e impostarlo su "ReadOnlyAccess". In questo modo gli utenti non potranno più scrivere nel bucket ONTAP S3.

Edit group

NAME

demo_s3_group

USERS

demo_s3_user ×

POLICIES

ReadOnlyAccess ×

Cancel

Save

Tutto ciò che resta da fare è configurare il DNS in modo che punti dal cluster ONTAP all'endpoint StorageGRID. Assicurarsi che il certificato dell'endpoint sia corretto e, se sono necessarie richieste di stile ospitate virtuali, aggiungere i nomi di dominio dell'endpoint in StorageGRID

Endpoint Domain Names

Virtual Hosted-Style Requests

Enable support of S3 virtual hosted-style requests by specifying API endpoint domain names. Support is disabled if this list is empty. Examples: s3.example.com, s3.example.co.uk, s3-east.example.com

Endpoint 1 +

I client dovranno attendere la scadenza del TTL o scaricare il DNS per risolvere il problema nel nuovo sistema in modo da poter verificare che tutto funzioni. Resta solo ripulire le chiavi S3 temporanee iniziali utilizzate per verificare l'accesso ai dati StorageGRID (NON alle chiavi importate), rimuovere le relazioni SnapMirror e rimuovere i dati ONTAP.

Di Rafael Guedes e Aron Klein

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 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.