Report tecnici

StorageGRID solutions and resources

NetApp
December 12, 2025

Sommario

Report tecnici . . . 1
Introduzione ai report tecnici di StorageGRID . . . 1
NetApp StorageGRID e analisi dei big data . . . 1
Casi d'utilizzo di NetApp StorageGRID . . . 1
Perché scegliere StorageGRID per i data Lake? . . . 2
Benchmarking di Data warehouse e Lakehouses con storage a oggetti S3: Uno studio comparativo . . . 3
Tuning di Hadoop S3A . . . 6
Che cos'è Hadoop? . . . 6
HDFS Hadoop e connettore S3A . . . 6
Tuning del connettore Hadoop S3A . . . 7
TR-4871: Configurare StorageGRID per il backup e recovery con CommVault . . . 12
Eseguire backup e recovery di dati utilizzando StorageGRID e CommVault . . . 12
Panoramica della soluzione testata . . . 14
Guida al dimensionamento di StorageGRID . . . 16
Eseguire un lavoro di protezione dati . . . 18
Esaminare i test delle prestazioni di base . . . 27
Suggerimento del livello di coerenza della benna . . . 28
TR-4626: Bilanciatori del carico . . . 29
Utilizza sistemi di bilanciamento del carico di terze parti con StorageGRID . . . 29
Utilizzare i bilanciatori di carico StorageGRID . . . 30
Informazioni su come implementare i certificati SSL per HTTPS in StorageGRID . . . 31
Configurare il bilanciamento del carico di terze parti attendibile in StorageGRID . . . 32
Informazioni sui bilanciatori del carico dei gestori del traffico locali . . . 32
Scopri i pochi casi di utilizzo per le configurazioni StorageGRID . . . 36
Convalidare la connessione SSL in StorageGRID . . . 39
Comprendere i requisiti globali di bilanciamento del carico per StorageGRID . . . 39
TR-4645: Funzionalità di sicurezza . . . 40
Proteggi dati e metadati StorageGRID in un archivio di oggetti . . . 40
Funzioni di sicurezza per l'accesso ai dati . . . 42
Sicurezza di oggetti e metadati . . . 51
Funzioni di protezione di amministrazione . . . 53
Funzioni di sicurezza della piattaforma . . . 57
Integrazione del cloud . . . 59
TR-4921: Difesa dal ransomware . . . 60
Proteggere gli oggetti StorageGRID S3 dal ransomware . . . 60
Difesa dal ransomware tramite il blocco degli oggetti . . . 61
Difesa da ransomware tramite bucket replicati con versione . . . 64
Difesa dal ransomware tramite versione con policy IAM di protezione . . . 67
Indagine e bonifica del ransomware . . . 70
TR-4765: StorageGRID monitor . . . 72
Introduzione al monitoraggio StorageGRID . . . 72
Utilizzare il dashboard GMI per monitorare StorageGRID . . . 73
Utilizzare gli avvisi per monitorare StorageGRID . . . 74

Monitoraggio avanzato in StorageGRID . . . 75
Accedi alle metriche utilizzando Curl in StorageGRID . . . 78
Visualizza le metriche utilizzando la dashboard Grafana di StorageGRID . . . 79
Utilizzare i criteri di classificazione del traffico in StorageGRID . . . 80
Utilizzare i registri di controllo per monitorare StorageGRID . . . 83
USA l'app StorageGRID per Splunk . . . 83
TR-4882: Installazione di una griglia bare metal StorageGRID . . . 83
Introduzione all'installazione di StorageGRID . . . 83
Prerequisiti per l'installazione di StorageGRID . . . 84
Installa Docker per StorageGRID . . . 93
Preparare i file di configurazione dei nodi per StorageGRID . . . 93
Installare dipendenze e pacchetti StorageGRID . . . 97
Convalidare i file di configurazione di StorageGRID . . . 97
Avviare il servizio host StorageGRID . . . 99
Configurare il gestore di rete in StorageGRID . . . 99
Aggiungere i dettagli della licenza StorageGRID . . . 101
Aggiungere siti a StorageGRID . . . 102
Specificare le subnet di rete della griglia per StorageGRID . . . 103
Approva nodi griglia per StorageGRID . . . 104
Specificare i dettagli del server NTP per StorageGRID . . . 109
Specificare i dettagli del server DNS per StorageGRID . . . 110
Specificare le password di sistema per StorageGRID . . . 111
Rivedere la configurazione e completare l'installazione di StorageGRID . . . 112
Aggiorna i nodi bare-metal in StorageGRID . . . 114
TR-4907: Configurare StorageGRID con veritas Enterprise Vault . . . 115
Introduzione alla configurazione di StorageGRID per il failover del sito . . . 115
Configurare StorageGRID e veritas Enterprise Vault . . . 115
Configurare il blocco degli oggetti StorageGRID S3 per lo storage WORM . . . 121
Configurare il failover del sito StorageGRID per il disaster recovery . . . 125

Report tecnici

Introduzione ai report tecnici di StorageGRID

NetApp StorageGRID è una suite di storage a oggetti software-defined che supporta un'ampia gamma di casi di utilizzo in ambienti multicloud pubblici, privati e ibridi. StorageGRID offre il supporto nativo per l'API Amazon S3 e offre innovazioni leader del settore come la gestione automatica del ciclo di vita per memorizzare, proteggere, proteggere e conservare i dati non strutturati in modo conveniente per lunghi periodi.

StorageGRID fornisce documentazione relativa alle Best practice e ai consigli per diverse funzionalità e integrazioni di StorageGRID.

NetApp StorageGRID e analisi dei big data

Casi d'utilizzo di NetApp StorageGRID

La soluzione di storage a oggetti NetApp StorageGRID offre scalabilità, disponibilità dei dati, sicurezza e performance elevate. Le organizzazioni di ogni dimensione e settore utilizzano StorageGRID S3 per un'ampia gamma di casi d'utilizzo. Analizziamo alcuni scenari tipici:

Analisi dei big data: StorageGRID S3 viene spesso utilizzato come data Lake, dove le aziende memorizzano grandi quantità di dati strutturati e non strutturati per l'analisi utilizzando strumenti come Apache Spark, Splunk Smartstore e Dremio.

Tiering dati: i clienti NetApp utilizzano la funzionalità FabricPool di ONTAP per spostare automaticamente i dati tra un Tier locale ad alte prestazioni in StorageGRID. Il tiering libera il costoso storage flash per i dati hot, mantenendo i dati cold altamente disponibili su storage a oggetti a basso costo. Ciò massimizza performance e risparmi.

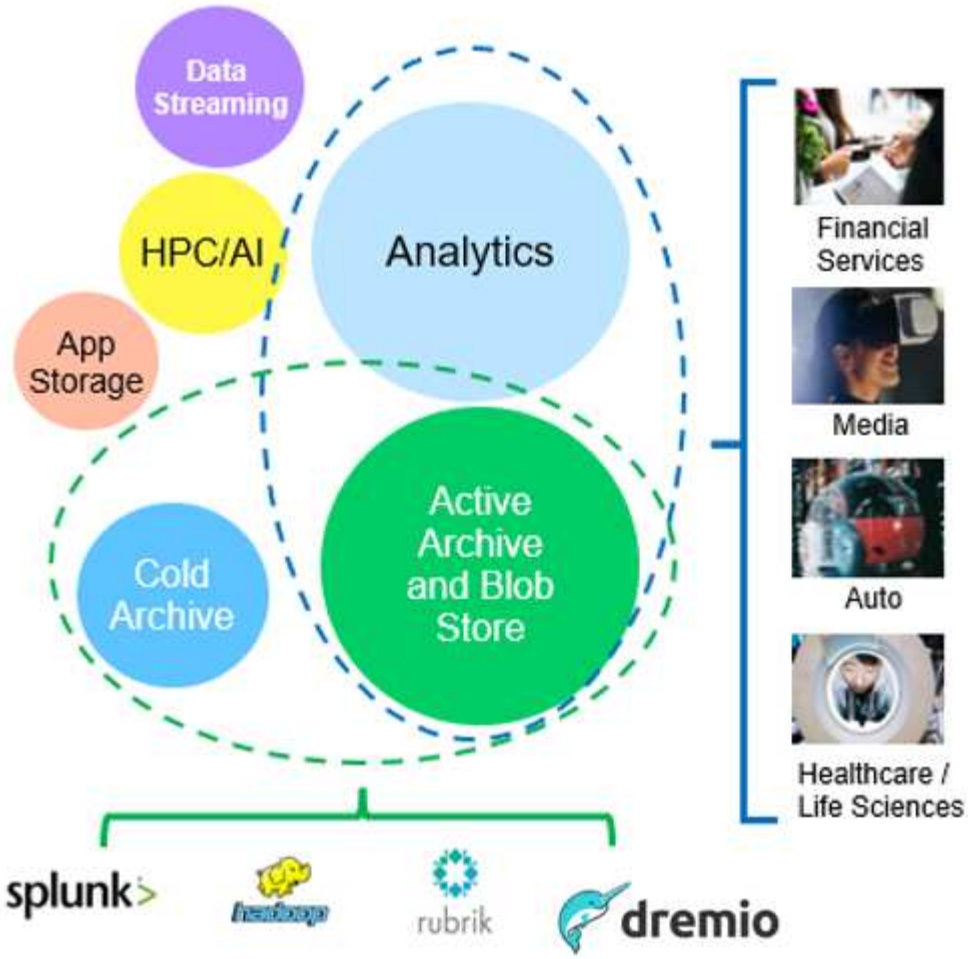
Backup dei dati e ripristino di emergenza: le aziende possono utilizzare StorageGRID S3 come soluzione affidabile e conveniente per il backup dei dati critici e il ripristino in caso di emergenza.

Archiviazione dei dati per le applicazioni: StorageGRID S3 può essere utilizzato come backend di archiviazione per le applicazioni, consentendo agli sviluppatori di archiviare e recuperare facilmente file, immagini, video e altri tipi di dati.

Distribuzione dei contenuti: StorageGRID S3 può essere utilizzato per archiviare e distribuire contenuti statici di siti web, file multimediali e download di software agli utenti di tutto il mondo, sfruttando la distribuzione geografica e lo spazio dei nomi globale di StorageGRID per una distribuzione dei contenuti rapida e affidabile.

Archivio dati: StorageGRID offre diversi tipi di storage e supporta il tiering in opzioni di storage pubblico a lungo termine a basso costo, rendendolo una soluzione ideale per l'archiviazione e la conservazione a lungo termine dei dati che devono essere conservati per scopi di conformità o cronologici.

Casi di utilizzo dello storage a oggetti

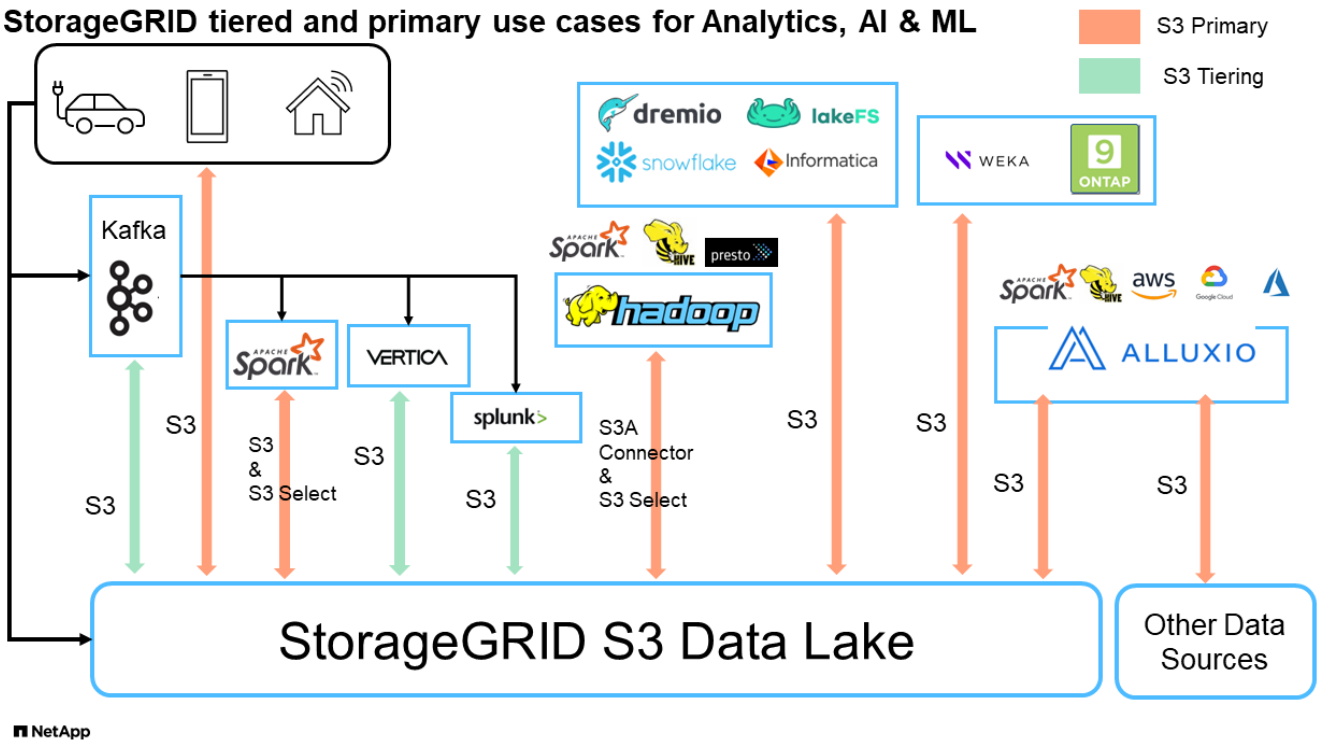


Tra questi, l'analisi dei big data è uno dei casi di utilizzo più importanti e l'andamento del suo utilizzo sta aumentando.

Perché scegliere StorageGRID per i data Lake?

- Maggiore collaborazione - massiccia condivisione multi-sito, multi-tenancy con accesso API standard del settore
- Costi operativi ridotti: Semplicità operativa di una singola architettura scale-out automatizzata con riparazione automatica
- Scalabilità: Diversamente dalle tradizionali soluzioni Hadoop e data warehouse, lo storage a oggetti StorageGRID S3 separa lo storage dalle risorse di calcolo e dai dati, consentendo al business di scalare le proprie esigenze di storage man mano che crescono.
- Durata e affidabilità: I StorageGRID offrono una durata del 99,999999999%, il che significa che i dati memorizzati sono altamente resistenti alla perdita di dati. Inoltre, offre un'elevata disponibilità per garantire che i dati siano sempre accessibili.
- Sicurezza: StorageGRID offre varie funzionalità di sicurezza, tra cui crittografia, policy per il controllo degli accessi, gestione del ciclo di vita dei dati, blocco degli oggetti e versioni per proteggere i dati archiviati in bucket S3

StorageGRID S3 Data Lake



Benchmarking di Data warehouse e Lakehouses con storage a oggetti S3: Uno studio comparativo

Questo articolo presenta un benchmark completo di vari ecosistemi di data warehouse e lakehouse che utilizzano NetApp StorageGRID. L'obiettivo è determinare il sistema che funziona meglio con lo storage a oggetti S3. Fare riferimento a questo "Apache Iceberg: La guida definitiva" per ulteriori informazioni sulle architetture datawarehous/lakehouse e sul formato tabella (Parquet e Iceberg).

- Strumento benchmark - TPC-DS - https://www.tpc.org/tpcds/
- Ecosistemi di big data
  - Cluster di macchine virtuali, ciascuno con 128G GB di RAM e 24 vCPU, storage SSD per disco di sistema
  - Hadoop 3.3.5 con Hive 3.1.3 (1 nodi nome + 4 nodi dati)
  - Delta Lake con Spark 3.2.0 (1 master + 4 dipendenti) e Hadoop 3.3.5
  - Dremio v25,2 (1 coordinatore + 5 esecutori)
  - Trino v438 (1 coordinatore + 5 lavoratori)
  - Starburst v453 (1 coordinatore + 5 lavoratori)
- Storage a oggetti
  - NetApp® StorageGRID^® 11,8 con bilanciamento del carico 3 x SG6060 + 1x SG1000
  - Protezione degli oggetti - 2 copie (il risultato è simile a EC 2+1)
- Dimensioni del database 1000GB
- La cache è stata disabilitata in tutti gli ecosistemi per ogni test di query utilizzando il formato Parquet. Per il formato Iceberg, abbiamo confrontato il numero di richieste GET S3 e il tempo totale di query tra scenari con cache disabilitata e scenari con cache abilitata.

TPC-DS include 99 query SQL complesse progettate per il benchmarking. Abbiamo misurato il tempo totale impiegato per eseguire tutte le 99 query e abbiamo condotto un'analisi dettagliata esaminando il tipo e il numero di richieste S3. I nostri test hanno confrontato l'efficienza di due formati di tabella popolari: Parquet e Iceberg.

Risultato query TPC-DS con formato tabella parquet

Ecosistema	Alveare	Lago Delta	Dremio	Trino	Starburst
TPCDS 99 query minuti totali	1084 [1]	55	36	32	28
S3 richieste di ripartizione	OTTIENI	1.117.184	2.074.610	3.939.690	1.504.212
1.495.039	osservazione: Tutta la gamma	80% range get di 2KB a 2MB da 32MB oggetti, 50 - 100 richieste/sec	Il range del 73% è inferiore a 100KB da 32MB oggetti, 1000 - 1400 richieste/sec	90% 1M byte range get from 256MB objects, 2500 - 3000 requests/sec	Dimensioni del range: 50% inferiore a 100KB, 16% circa 1MB, 27% 2MB-9MB, 3500 - 4000 richieste/sec
Dimensioni del range: 50% inferiore a 100KB, 16% circa 1MB, 27% 2MB-9MB, 4000 - 5000 richiesta/sec	Elenca oggetti	312.053	24.158	120	509
512	TESTA (oggetto inesistente)	156.027	12.103	96	0
0	TESTA (oggetto esistente)	982.126	922.732	0	0
0	Richieste totali	2.567.390	3.033.603	3.939,906	1.504.721

[1] Impossibile completare la query numero 72

Risultato query TPC-DS con formato tabella Iceberg

Ecosistema	Dremio	Trino	Starburst
TPCDS 99 query + minuti totali (cache disattivata)	22	28	22
TPCDS 99 query + minuti totali [2] (cache abilitata)	16	28	21,5
S3 richieste di ripartizione	GET (OTTIENI) (cache disattivata)	1.985.922	938.639
931.582	GET (OTTIENI) (cache abilitata)	611.347	30.158
3.281	osservazione: Tutta la gamma	Dimensioni di RICEZIONE intervallo: 67% 1MB, 15% 100KB, 10% 500KB, 3500 - 4500 richieste/sec	Dimensioni del range: 42% inferiore a 100KB, 17% circa 1MB, 33% 2MB-9MB, 3500 - 4000 richieste/sec
Dimensioni del range: 43% inferiore a 100KB, 17% circa 1MB, 33% 2MB-9MB, 4000 - 5000 richieste/sec	Elenca oggetti	1465	0
0	TESTA (oggetto inesistente)	1464	0
0	TESTA (oggetto esistente)	3.702	509
509	Richieste totali (cache disattivata)	1.992.553	939.148

[2] le prestazioni Trino/Starburst sono causate da colli di bottiglia causati dalle risorse di elaborazione; l'aggiunta di più RAM al cluster riduce il tempo totale di query.

Come mostrato nella prima tabella, Hive è significativamente più lento di altri moderni dati ecosistemi lakehouse. Abbiamo osservato che Hive ha inviato un gran numero di richieste list-objects S3, che in genere sono lente su tutte le piattaforme di storage a oggetti, soprattutto quando si gestiscono bucket contenenti molti oggetti. Ciò aumenta notevolmente la durata complessiva della query. Inoltre, i moderni ecosistemi lakehouse possono inviare in parallelo un elevato numero di richieste GET, che vanno da 2.000 a 5.000 richieste al secondo, rispetto alle richieste da 50 a 100 di Hive al secondo. Il file system standard mimicry di Hive e Hadoop S3A contribuisce alla lentezza di Hive nell'interazione con lo storage a oggetti S3.

L'utilizzo di Hadoop (su storage a oggetti HDFS o S3) con Hive o Spark richiede un'estesa conoscenza di Hadoop e Hive/Spark, oltre a una comprensione dell'interazione delle impostazioni di ogni servizio. Insieme, hanno più di 1.000 impostazioni, molte delle quali sono correlate e non possono essere modificate indipendentemente. Trovare la combinazione ottimale di impostazioni e valori richiede un'enorme quantità di tempo e di lavoro.

Confrontando i risultati di Parquet e Iceberg, notiamo che il formato della tabella è un fattore di prestazioni importante. Il formato della tavola Iceberg è più efficiente del Parquet in termini di numero di S3 richieste, con

un numero di richieste inferiore dal 35% al 50% rispetto al formato Parquet.

Le prestazioni di Dremio, Trino o Starburst sono principalmente determinate dalla potenza di calcolo del cluster. Sebbene tutte e tre utilizzino il connettore S3A per la connessione allo storage a oggetti S3, non richiedono Hadoop e la maggior parte delle impostazioni fs.S3A di Hadoop non sono utilizzate da questi sistemi. Questo semplifica il tuning delle performance, eliminando la necessità di imparare e testare le varie impostazioni di Hadoop S3A.

Da questo risultato del benchmark, possiamo concludere che il sistema di analisi dei big data ottimizzato per carichi di lavoro basati su S3 è un importante fattore di performance. I moderni Lakehouse ottimizzano l'esecuzione delle query, utilizzano in modo efficiente i metadati e forniscono un accesso perfetto ai dati S3, producendo performance migliori rispetto a Hive quando si utilizza lo storage S3.

Fare riferimento a questa "pagina" sezione per configurare l'origine dati Dremio S3 con StorageGRID.

Visita i collegamenti riportati di seguito per scoprire come StorageGRID e Dremio collaborano per fornire un'infrastruttura di data Lake moderna ed efficiente e come NetApp è passata da Hive + HDFS a Dremio + StorageGRID per migliorare in modo significativo l'efficienza dell'analisi dei big data.

- "Migliora le performance dei tuoi big data con NetApp StorageGRID"
- "Infrastruttura di data Lake moderna, potente ed efficiente con StorageGRID e Dremio"
- "In che modo NetApp sta ridefinendo l'esperienza del cliente con l'analisi dei prodotti"

Tuning di Hadoop S3A

Di Angela Cheng

Il connettore Hadoop S3A facilita un'interazione perfetta tra le applicazioni basate su Hadoop e lo storage a oggetti S3. La messa a punto del connettore Hadoop S3A è essenziale per ottimizzare le performance quando si lavora con lo storage a oggetti S3. Prima di entrare nei dettagli di messa a punto, cerchiamo di comprendere di base Hadoop e i suoi componenti.

Che cos'è Hadoop?

Hadoop è un potente framework open-source progettato per gestire l'elaborazione e lo storage di dati su larga scala. Permette lo storage distribuito e l'elaborazione parallela tra cluster di computer.

I tre componenti principali di Hadoop sono:

- **Hadoop HDFS (Hadoop Distributed file System)**: Gestisce lo storage, suddividendo i dati in blocchi e distribuendoli tra i nodi.
- **Hadoop MapReduce**: Responsabile dell'elaborazione dei dati dividendo le attività in blocchi più piccoli ed eseguendole in parallelo.
- **Hadoop YARN (Yet Another Resource negoziator):** "Gestisce le risorse e pianifica le attività in modo efficiente"

HDFS Hadoop e connettore S3A

HDFS è una componente vitale dell'ecosistema Hadoop, ricoprendo un ruolo critico nell'efficiente elaborazione dei big data. HDFS consente storage e gestione affidabili. Garantisce l'elaborazione parallela e lo storage dei dati ottimizzato, accelerando l'accesso e l'analisi dei dati.

Nell'elaborazione dei big data, HDFS è eccellente per fornire storage con tolleranza di errore per grandi set di dati. Ottiene questo attraverso la replica dei dati. Consente di memorizzare e gestire grandi volumi di dati strutturati e non strutturati in un ambiente di data warehouse. Inoltre, si integra perfettamente con i principali framework di elaborazione dei big data, come Apache Spark, Hive, Pig e Flink, consentendo un'elaborazione dei dati scalabile ed efficiente. È compatibile con i sistemi operativi basati su Unix (Linux), il che lo rende la scelta ideale per le organizzazioni che preferiscono utilizzare ambienti basati su Linux per l'elaborazione dei big data.

Con la crescita del volume dei dati nel tempo, l'approccio all'aggiunta di nuove macchine al cluster Hadoop con risorse di calcolo e storage proprie è diventato inefficiente. La scalabilità lineare crea delle sfide per l'utilizzo efficiente delle risorse e la gestione dell'infrastruttura.

Per affrontare queste sfide, il connettore Hadoop S3A offre i/o dalle performance elevate rispetto allo storage a oggetti S3. L'implementazione di un workflow Hadoop con S3A consente di sfruttare lo storage a oggetti come repository di dati e consente di separare calcolo e storage, il che consente di scalare calcolo e storage in modo indipendente. Il disaccoppiamento tra calcolo e storage ti consente inoltre di dedicare la giusta quantità di risorse per i tuoi job di calcolo e di fornire capacità in base alle dimensioni del set di dati. Pertanto, è possibile ridurre il TCO complessivo per i flussi di lavoro Hadoop.

Tuning del connettore Hadoop S3A

S3 si comporta in modo diverso da HDFS e alcuni tentativi di preservare l'aspetto di un file system sono decisamente non ottimali. È necessario un'accurata messa a punto/test/sperimentazione per utilizzare al meglio le risorse S3.

Le opzioni Hadoop di questo documento si basano su Hadoop 3,3.5, fare riferimento a. "Hadoop 3.3.5 core-site.xml" per tutte le opzioni disponibili.

Nota – il valore predefinito di alcune impostazioni di Hadoop fs.S3A è diverso in ogni versione di Hadoop. Assicurati di controllare il valore predefinito specifico per la tua attuale versione di Hadoop. Se queste impostazioni non sono specificate in Hadoop core-site.xml, verrà utilizzato il valore predefinito. È possibile ignorare il valore in fase di esecuzione utilizzando le opzioni di configurazione Spark o Hive.

Dovete andare a questo "Pagina di Apache Hadoop" per capire ogni opzione fs.s3a. Se possibile, testarle in un cluster Hadoop non di produzione per trovare i valori ottimali.

Si dovrebbe leggere "Ottimizzazione delle prestazioni quando si lavora con il connettore S3A" per altre raccomandazioni di sintonizzazione.

Analizziamo alcune considerazioni chiave:

1. Compressione dati

Non attivare la compressione StorageGRID. La maggior parte dei sistemi di big data utilizza la funzione GET della gamma di byte invece di recuperare l'intero oggetto. L'utilizzo dell'intervallo di byte Get con gli oggetti compressi riduce significativamente le prestazioni di GET.

2. S3A committer

In generale, si raccomanda il committer Magic S3A. Fare riferimento a questo "Pagina delle opzioni comuni di committer S3A" per avere una migliore comprensione di magic committer e delle relative impostazioni s3a.

Magic Committer:

Magic Committer si affida specificamente a S3Guard per offrire elenchi di directory coerenti sull'archivio di

oggetti S3.

Con S3 coerente (che è ora il caso), il Magic Committer può essere utilizzato in modo sicuro con qualsiasi secchio S3.

Scelta e sperimentazione:

A seconda del caso d'uso, è possibile scegliere tra il committer di staging (che si basa su un filesystem HDFS del cluster) e il committer magico.

Sperimenta entrambi per determinare la soluzione più adatta al tuo carico di lavoro e ai requisiti.

In sintesi, i S3A committer forniscono una soluzione alla sfida fondamentale di un impegno coerente, ad alte prestazioni e affidabile nei confronti del S3. Il design interno garantisce un trasferimento efficiente dei dati, mantenendo al contempo l'integrità dei dati.

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.committer.name	Committer to create for output to S3A, one of: "file", "directory", "partitioned", "magic".	file
fs.s3a.buffer.dir	Local filesystem directory for data being written and/or staged.	${env.LOCAL_DIRS:-${hadoop.tmp.dir}}/s3a
fs.s3a.committer.magic.enabled	Enable "magic committer" support in the filesystem.	true
fs.s3a.committer.abort.pending.uploads	list and abort all pending uploads under the destination path when the job is committed or aborted.	true
fs.s3a.committer.threads	Number of threads in committers for parallel operations on files.	8
fs.s3a.committer.generate.uuid	Generate a Job UUID if none is passed down from Spark	false
fs.s3a.committer.require.uuid	Require the Job UUID to be passed down from Spark	false
mapreduce.fileoutputcommitter.marksuccessfuljobs	Write a _SUCCESS file on the successful completion of the job.	true
mapreduce.outputcommitter.factory.scheme.s3a	The committer factory to use when writing data to S3A filesystems. If mapreduce.outputcommitter.factory.class is set, it will override this property. (This property is set in mapred-default.xml)	org.apache.hadoop.fs.s3a.commit.S3ACommitterFactory

3. Filettatura, dimensioni pool di connessione e dimensione blocco

- Ogni client **S3A** che interagisce con un singolo bucket ha un proprio pool dedicato di connessioni HTTP 1,1 aperte e thread per operazioni di upload e copia.
- "È possibile ottimizzare le dimensioni di questi pool per ottenere un equilibrio tra prestazioni e utilizzo di memoria/thread".
- Quando si caricano i dati su S3, questi vengono divisi in blocchi. La dimensione predefinita del blocco è 32 MB. È possibile personalizzare questo valore impostando la proprietà fs.S3A.block.size.
- Blocchi di dimensioni maggiori possono migliorare le performance per il caricamento di grandi dati, riducendo l'overhead di gestione di parti multiparte durante il caricamento. Il valore consigliato è pari o superiore a 256 MB per set di dati di grandi dimensioni.

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.threads.max	The total number of threads available in the filesystem for data uploads *or any other queued filesystem operation*.	64
fs.s3a.connection.maximum	Controls the maximum number of simultaneous connections to S3. This must be bigger than the value of fs.s3a.threads.max so as to stop threads being blocked waiting for new HTTPS connections. Why not equal? The AWS SDK transfer manager also uses these connections.	96
fs.s3a.max.total.tasks	The number of operations which can be queued for execution. This is in addition to the number of active threads in fs.s3a.threads.max.	32
fs.s3a.committer.threads	Number of threads in committers for parallel operations on files (upload, commit, abort, delete...)	8
fs.s3a.executor.capacity	The maximum number of submitted tasks which is a single operation (e.g. rename(), delete()) may submit simultaneously for execution -excluding the IO-heavy block uploads, whose capacity is set in "fs.s3a.fast.upload.active.blocks" All tasks are submitted to the shared thread pool whose size is set in "fs.s3a.threads.max"; the value of capacity should be less than that of the thread pool itself, as the goal is to stop a single operation from overloading that thread pool.	16
fs.s3a.fast.upload.active.blocks (see also related fs.s3a.fast.upload.buffer option)	Maximum Number of blocks a single output stream can have active (uploading, or queued to the central FileSystem instance's pool of queued operations. This stops a single stream overloading the shared thread pool.	4
fs.s3a.block.size	Block size to use when reading files using s3a: file system. A suffix from the set {K,M,G,T,P} may be used to scale the numeric value.	32MB (tested 1TB data set with 256MB and 512MB block size shows significant improvement in both read and write)

4. Caricamento multiparte

S3A committer **Always** utilizza MPU (upload multiparte) per caricare i dati nel bucket S3. Ciò è necessario per consentire: Errore di attività, esecuzione speculativa di attività e interruzione di processi prima del commit. Di seguito sono riportate alcune specifiche chiave relative ai caricamenti di più parti:

- Dimensioni massime oggetto: 5 TiB (terabyte).
- Numero massimo di parti per caricamento: 10.000.
- Numeri di parte: Da 1 a 10.000 (inclusi).
- Dimensioni del pezzo: Tra 5 MIB e 5 GiB. In particolare, non esiste un limite minimo di dimensioni per l'ultima parte del caricamento multiparte.

L'utilizzo di una parte di dimensioni inferiori per i caricamenti multiparte S3 presenta vantaggi e svantaggi.

Vantaggi:

- Ripristino rapido da problemi di rete: Quando si caricano parti più piccole, l'impatto del riavvio di un caricamento non riuscito a causa di un errore di rete viene ridotto al minimo. Se una parte non riesce, è sufficiente caricare nuovamente quella parte specifica piuttosto che l'intero oggetto.

- Migliore parallelizzazione: È possibile caricare più parti in parallelo, sfruttando il multithreading o le connessioni simultanee. Questa parallelizzazione migliora le prestazioni, soprattutto quando si gestiscono file di grandi dimensioni.

Svantaggio:

- Sovraccarico di rete: Le dimensioni ridotte delle parti consentono il caricamento di più parti, ciascuna delle quali richiede una propria richiesta HTTP. Un numero maggiore di richieste HTTP aumenta l'overhead dovuto all'avvio e al completamento di singole richieste. La gestione di un gran numero di piccoli componenti può influire sulle prestazioni.
- Complessità: Gestire l'ordine, tenere traccia delle parti e assicurarsi che i caricamenti vengano effettuati correttamente può risultare difficoltoso. Se il caricamento deve essere interrotto, tutte le parti già caricate devono essere monitorate e eliminate.

Per Hadoop, per fs.S3A.multipart.size si consigliano dimensioni di parte pari o superiori a 256MB. Impostare sempre il valore fs.S3A.mutlipart.threshold su 2 x fs.S3A.multipart.size. Ad esempio, se fs.S3A.multipart.size = 256M, fs.S3A.mutlipart.threshold dovrebbe essere 512M.

Utilizzare parti di dimensioni maggiori per set di dati di grandi dimensioni. È importante scegliere una dimensione della parte che bilanci questi fattori in base al caso di utilizzo specifico e alle condizioni di rete.

Un caricamento multiparte è un "processo in tre fasi":

1. Il caricamento viene avviato, StorageGRID restituisce un ID upload.
2. Le parti dell'oggetto vengono caricate utilizzando l'ID upload.
3. Una volta caricate tutte le parti dell'oggetto, invia la richiesta di caricamento multiparte completa con upload-ID. StorageGRID costruisce l'oggetto dalle parti caricate e il client può accedere all'oggetto.

Se la richiesta di caricamento multiparte completa non viene inviata correttamente, le parti rimangono in StorageGRID e non creano alcun oggetto. Ciò si verifica quando i lavori vengono interrotti, non riusciti o interrotti. Le parti rimangono nella griglia fino a quando il caricamento multiparte non viene completato o interrotto o StorageGRID elimina queste parti se sono trascorsi 15 giorni dall'avvio del caricamento. Se in un bucket sono presenti molti (da poche centinaia di migliaia a milioni) upload multiparte in corso, quando Hadoop invia "list-multipart-Uploads" (questa richiesta non filtra per id di caricamento), il completamento della richiesta potrebbe richiedere molto tempo o un timeout. È possibile impostare fs.S3A.mutlipart.purge su true con un valore fs.S3A.multipart.purge.age appropriato (ad esempio, da 5 a 7 giorni, non utilizzare il valore predefinito di 86400, ossia 1 giorno). O contattare l'assistenza NetApp per esaminare la situazione.

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.multipart.size	How big (in bytes) to split upload or copy operations up into. A suffix from the set {K,M,G,T,P} may be used to scale the numeric value.	64M
fs.s3a.multipart.threshold	How big (in bytes) to split upload or copy operations up into. This also controls the partition size in renamed files, as rename() involves copying the source file(s). A suffix from the set {K,M,G,T,P} may be used to scale the numeric value.	128M
fs.s3a.multipart.purge	True if you want to purge existing multipart uploads that may not have been completed/aborted correctly. The corresponding purge age is defined in fs.s3a.multipart.purge.age. If set, when the filesystem is instantiated then all outstanding uploads older than the purge age will be terminated -across the entire bucket. This will impact multipart uploads by other applications and users. so should be used sparingly, with an age value chosen to stop failed uploads, without breaking ongoing operations.	false
fs.s3a.multipart.purge.age	Minimum age in seconds of multipart uploads to purge on startup if "fs.s3a.multipart.purge" is true	86400

5. Buffer: Scrittura dei dati in memoria

Per migliorare le prestazioni, è possibile inserire i dati in scrittura nella memoria prima di caricarli su S3. Riducendo così il numero di scritture ridotte e migliorando l'efficienza.

Option	Meaning	Default (Hadoop 3.3.5)
fs.s3a.fast.upload.buffer	The buffering mechanism to for data being written. Values: disk, array, bytebuffer. "disk" will use the directories listed in fs.s3a.buffer.dir as the location(s) to save data prior to being uploaded. "array" uses arrays in the JVM heap "bytebuffer" uses off-heap memory within the JVM. Both "array" and "bytebuffer" will consume memory in a single stream up to the number of blocks set by: fs.s3a.multipart.size * fs.s3a.fast.upload.active.blocks. If using either of these mechanisms, keep this value low The total number of threads performing work across all threads is set by fs.s3a.threads.max, with fs.s3a.max.total.tasks values setting the number of queued work items.	disk

Ricorda che S3 e HDFS funzionano in modi diversi. È necessario un'attenta messa a punto/test/esperimento

per utilizzare al meglio le risorse S3.

TR-4871: Configurare StorageGRID per il backup e recovery con CommVault

Eseguire backup e recovery di dati utilizzando StorageGRID e CommVault

CommVault e NetApp hanno collaborato alla creazione di una soluzione congiunta per la data Protection, che combina il software CommVault complete Backup and Recovery for NetApp con il software NetApp StorageGRID per il cloud storage. CommVault complete Backup and Recovery e NetApp StorageGRID forniscono soluzioni uniche e facili da utilizzare che collaborano per aiutarti a soddisfare le richieste di una rapida crescita dei dati e delle normative in aumento in tutto il mondo.

Molte organizzazioni vogliono migrare lo storage nel cloud, scalare i sistemi e automatizzare la policy per la conservazione dei dati a lungo termine. Lo storage a oggetti basato sul cloud è celebre per la sua resilienza, la sua capacità di scalare e le efficienze operative e legate ai costi, caratteristiche che lo rendono la scelta naturale come destinazione del backup. CommVault e NetApp hanno certificato congiuntamente la propria soluzione combinata nel 2014 e da allora hanno progettato una più profonda integrazione tra le due soluzioni. I clienti di ogni tipo in tutto il mondo hanno adottato la soluzione combinata di backup e recovery CommVault complete e StorageGRID.

Informazioni su CommVault e StorageGRID

Il software CommVault complete Backup and Recovery è una soluzione di gestione integrata dei dati e delle informazioni di livello aziendale, costruita da zero su una singola piattaforma e con una base di codice unificata. Tutte le sue funzioni condividono tecnologie di back-end, apportando gli impareggiabili vantaggi e vantaggi di un approccio completamente integrato alla protezione, alla gestione e all'accesso ai dati. Il software contiene moduli per la protezione, l'archiviazione, l'analisi, la replica e la ricerca dei dati. I moduli condividono una serie comune di servizi back-end e funzionalità avanzate che interagiscono perfettamente tra loro. La soluzione affronta tutti gli aspetti della gestione dei dati nell'azienda, fornendo una scalabilità infinita e un controllo senza precedenti di dati e informazioni.

NetApp StorageGRID come Tier di cloud CommVault è una soluzione di storage a oggetti di cloud ibrido aziendale. Puoi implementarla su più siti, sia su un'appliance costruita ad hoc che come implementazione software-defined. StorageGRID ti consente di stabilire policy di gestione dei dati che determinano il modo in cui i dati vengono archiviati e protetti. StorageGRID raccoglie le informazioni necessarie per sviluppare e applicare le policy. Prende in esame un'ampia gamma di caratteristiche ed esigenze, tra cui performance, durata, disponibilità, posizione geografica, longevità e costi. I dati sono pienamente mantenuti e protetti durante lo spostamento tra posizioni e man mano che invecchiano.

Il motore di policy intelligente di StorageGRID consente di scegliere una delle seguenti opzioni:

- Utilizzare l'erasure coding per eseguire il backup dei dati su diversi siti allo scopo di ottenere resilienza.
- Copia degli oggetti in siti remoti per ridurre al minimo il costo e la latenza della WAN.

Quando StorageGRID archivia un oggetto, lo accedi come un unico oggetto, indipendentemente da dove si trova o dal numero di copie esistenti. Questo comportamento è fondamentale per il disaster recovery, perché con esso, anche se una copia di backup dei dati è danneggiata, StorageGRID è in grado di ripristinare i dati.

Conservare i dati di backup nello storage primario può rivelarsi costoso. Utilizzando NetApp StorageGRID, potrai liberare spazio sullo storage primario migrando i dati di backup inattivi in StorageGRID, senza rinunciare

alle numerose funzionalità di StorageGRID. Il valore dei dati di backup cambia con il passare del tempo, così come il costo legato alla loro memorizzazione. StorageGRID può ridurre al minimo il costo dello storage primario aumentando al contempo la durata dei dati.

Funzionalità principali

Le funzionalità principali della piattaforma software CommVault includono:

- Una soluzione completa di protezione dei dati che supporta tutti i principali sistemi operativi, database e applicazioni su server virtuali e fisici, sistemi NAS, infrastrutture basate sul cloud e dispositivi mobili.
- Gestione semplificata attraverso un'unica console: Puoi visualizzare, gestire e accedere a tutte le funzioni, tutti i dati e le informazioni dell'azienda.
- Diversi metodi di protezione, tra cui backup e archiviazione dei dati, gestione delle snapshot, replica dei dati e indicizzazione dei contenuti per l'e-Discovery.
- Gestione efficiente dello storage mediante la deduplica per il disco e il cloud storage.
- Integrazione con storage array NetApp come AFF, FAS, NetApp HCI ed e-Series e con i sistemi di storage scale-out NetApp SolidFire^®. Integrazione anche con il software NetApp Cloud Volumes ONTAP per automatizzare la creazione di copie Snapshot™ NetApp indicizzate e compatibili con le applicazioni nell'intero portafoglio di storage NetApp.
- Gestione completa dell'infrastruttura virtuale che supporta i principali hypervisor virtuali on-premise e piattaforme hyperscaler di cloud pubblico.
- Funzionalità di sicurezza avanzate per limitare l'accesso ai dati critici, offrire funzionalità di gestione granulari e fornire accesso single-sign-on agli utenti di Active Directory.
- Gestione dei dati basata su criteri che consente di gestire i dati in base alle esigenze aziendali, non in base a una posizione fisica.
- Un'esperienza utente finale all'avanguardia, che consente agli utenti di proteggere, trovare e ripristinare i propri dati.
- Automazione basata su API per utilizzare strumenti di terze parti come vRealize Automation o Service Now per gestire le operazioni di data Protection e recovery.

Per ulteriori informazioni sui carichi di lavoro supportati, visitare il sito Web "Tecnologie supportate da CommVault".

Opzioni di backup

Quando implementi il software di backup e recovery CommVault complete con il cloud storage, hai due opzioni di backup:

- Eseguire il backup su una destinazione disco primaria e una copia ausiliaria su cloud storage.
- Eseguire il backup sul cloud storage come destinazione primaria.

In passato, lo storage a oggetti o cloud era considerato dalle performance troppo basse per essere utilizzato per il backup primario. L'utilizzo di una destinazione disco primaria ha permesso ai clienti di disporre di processi di backup e ripristino più rapidi e di mantenere una copia ausiliaria nel cloud come backup cold. StorageGRID rappresenta la nuova generazione dello storage a oggetti. StorageGRID è in grado di offrire performance elevate, throughput elevato, performance e flessibilità superiori a quelle degli altri vendor di soluzioni storage a oggetti.

Nella seguente tabella sono elencati i vantaggi di ciascuna opzione di backup con StorageGRID:

	Backup primario su disco e copia ausiliaria su StorageGRID	Backup primario su StorageGRID
Performance	Tempo di recovery più rapido, con montaggio live o live recovery: La soluzione migliore per i carichi di lavoro Tier0/Tier1.	Non può essere utilizzato per operazioni di montaggio live o ripristino live. Ideale per le operazioni di ripristino in streaming e per la conservazione a lungo termine.
Architettura di implementazione	Utilizzo di una tecnologia all-flash o di un disco a rotazione come primo landing Tier di backup. StorageGRID viene utilizzato come Tier secondario.	Semplifica l'implementazione utilizzando StorageGRID come destinazione di backup all-inclusive.
Funzioni avanzate (ripristino in tempo reale)	Supportato	Non supportato

Dove trovare ulteriori informazioni

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

- Centro di documentazione di StorageGRID 11,9 + https://docs.netapp.com/us-en/storagegrid-119/
- Documentazione del prodotto NetApp https://docs.netapp.com
- Documentazione CommVault https://documentation.commvault.com/2024/essential/index.html

Panoramica della soluzione testata

La soluzione collaudata combina le soluzioni CommVault e NetApp per realizzare una potente soluzione congiunta.

Setup della soluzione

Durante la configurazione in laboratorio, l'ambiente StorageGRID era composto da quattro appliance NetApp StorageGRID SG5712, un nodo amministrativo primario virtuale e un nodo gateway virtuale. L'appliance SG5712 è l'opzione entry-level, una configurazione di base. La scelta di opzioni dalle performance più elevate come NetApp StorageGRID SG5760 o SG6060 può fornire benefici significativi in termini di performance. Per assistenza sul dimensionamento, consulta il Solution Architect NetApp StorageGRID.

Per la policy di protezione dei dati, StorageGRID utilizza una policy di Lifecycle management integrata (ILM) per gestire e proteggere i dati. Le regole ILM vengono valutate in una politica dall'alto verso il basso. Il criterio ILM viene implementato come illustrato nella tabella seguente:

Regola ILM	Qualificatori	Comportamento di acquisizione
Erasure coding 2+1	Oggetti superiori a 200KB	Bilanciato

Regola ILM	Qualificatori	Comportamento di acquisizione
2 Copia	Tutti gli oggetti	Dual commit

La regola di copia di ILM 2 è la regola predefinita. La regola Erasure Coding 2+1 è stata applicata per questo test a qualsiasi oggetto 200KB o superiore. La regola predefinita è stata applicata agli oggetti di dimensioni inferiori a 200KB. L'applicazione delle regole in questo modo è una Best practice di StorageGRID.

Per informazioni tecniche su questo ambiente di test, leggere la sezione progettazione della soluzione e Best practice nella "Data Protection scale-out NetApp con CommVault" report tecnico.

Specifiche dell'hardware StorageGRID

La tabella seguente descrive l'hardware NetApp StorageGRID utilizzato per questo test. L'appliance StorageGRID SG5712 con connettività di rete 10Gbps è l'opzione entry-level e rappresenta una configurazione di base. In alternativa, SG5712 può essere configurato per il collegamento in rete 25Gbps.

Hardware	Quantità	Disco	Capacità utilizzabile	Rete
Appliance StorageGRID SG5712	4	48 x 4TB GB (HDD SAS near-line)	136TB	10Gbps

La scelta di opzioni di appliance con performance più elevate come le appliance NetApp StorageGRID SG5760, SG6060 o All Flash SGF6112 può fornire benefici significativi in termini di performance. Per assistenza sul dimensionamento, consulta il Solution Architect NetApp StorageGRID.

Requisiti software CommVault e StorageGRID

Le tabelle seguenti elencano i requisiti software per il software CommVault e NetApp StorageGRID installato sul software VMware ai fini del test. Sono stati installati quattro programmi di gestione della trasmissione dati MediaAgent e un server CommServe. Nel test è stata implementata la connettività di rete 10Gbps per l'infrastruttura VMware. La tabella seguente

La tabella seguente elenca i requisiti di sistema totali del software CommVault:

Componente	Quantità	Datastore	Dimensione	Totale	Numero totale di IOPS richiesti
CommServe Server	1	SISTEMA OPERATIVO	500GB	500GB	n/a.
		SQL	500GB	500GB	n/a.
MediaAgent	4	CPU virtuale (vCPU)	16	64	n/a.
		RAM	128GB	512	n/a.

Componente	Quantità	Datastore	Dimensione	Totale	Numero totale di IOPS richiesti
		SISTEMA OPERATIVO	500GB	2TB	n/a.
		Cache indice	2TB	8TB	200+
		DB	2TB	8TB	200-80.000K

Nell'ambiente di test, sono stati implementati un nodo di amministrazione principale virtuale e un nodo di gateway virtuale su VMware su uno storage array NetApp e-Series E2812. Ciascun nodo si trovava su un server separato con i requisiti minimi dell'ambiente di produzione descritti nella tabella seguente:

Nella tabella seguente sono elencati i requisiti per i nodi amministrativi virtuali StorageGRID e i nodi gateway:

Tipo di nodo	Quantità	VCPU	RAM	Storage
Nodo gateway	1	8	24GB	100GB LUN per il sistema operativo
Nodo amministrativo	1	8	24GB	100GB LUN per il sistema operativo 200GB LUN per le tabelle dei nodi Admin 200GB LUN per l'audit log del nodo Admin

Guida al dimensionamento di StorageGRID

Consulta i tuoi specialisti in materia di data Protection NetApp per dimensionamento specifico del tuo ambiente. Gli specialisti della data Protection di NetApp possono utilizzare lo strumento CommVault Total Backup Storage Calculator per stimare i requisiti dell'infrastruttura di backup. Lo strumento richiede l'accesso al portale per i partner CommVault. Se necessario, registrati per accedere.

Input per il dimensionamento di CommVault

È possibile utilizzare le seguenti attività per eseguire il rilevamento per il dimensionamento della soluzione per la data Protection:

- Identifica i carichi di lavoro del sistema o dell'applicazione/database e la capacità front-end corrispondente (in terabyte [TB]) da proteggere.
- Identifica il carico di lavoro VM/file e la capacità front-end (TB) simile che deve essere protetta.
- Identificare i requisiti di conservazione a breve e a lungo termine.

- Identificare il change rate quotidiano in % per i set di dati/carichi di lavoro identificati.
- Identificazione della crescita dei dati prevista nei prossimi 12, 24 e 36 mesi.
- Definisci RTO e RPO per la data Protection/recovery in base alle esigenze di business.

Quando queste informazioni sono disponibili, è possibile eseguire il dimensionamento dell'infrastruttura di backup in modo da suddividere le capacità di storage richieste.

Guida al dimensionamento di StorageGRID

Prima di eseguire il dimensionamento del NetApp StorageGRID, prendi in considerazione questi aspetti del carico di lavoro:

- Capacità utilizzabile
- Modalità WORM
- Dimensione media dell'oggetto
- Requisiti relativi alle performance
- Criterio ILM applicato

La quantità di capacità utilizzabile ha bisogno di per adattarsi alla dimensione del workload di backup su cui si è eseguito il tiering in StorageGRID e al programma di conservazione.

La modalità WORM sarà attivata o meno? Una volta abilitato WORM in CommVault, il blocco degli oggetti verrà configurato su StorageGRID. In questo modo si aumenterà la capacità dello storage a oggetti necessaria. La quantità di capacità richiesta varia in base alla durata di conservazione e al numero di modifiche agli oggetti per ogni backup.

Average object size è un parametro di input che aiuta nel dimensionamento delle performance in un ambiente StorageGRID. Le dimensioni medie degli oggetti utilizzate per un carico di lavoro CommVault dipendono dal tipo di backup.

La tabella seguente elenca le dimensioni medie degli oggetti per tipo di backup e descrive le letture del processo di ripristino dall'archivio di oggetti:

Tipo di backup	Dimensione media oggetto	Ripristinare il comportamento
Eseguire una copia ausiliaria in StorageGRID	32MB	Lettura completa dell'oggetto 32MB
Backup diretto su StorageGRID (deduplica abilitata)	8MB	1MB lettura casuale
Backup diretto su StorageGRID (deduplica disattivata)	32MB	Lettura completa dell'oggetto 32MB

Inoltre, la comprensione dei requisiti prestazionali per backup completi e backup incrementali consente di determinare il dimensionamento dei nodi di storage StorageGRID. I metodi di data Protection della policy ILM (Information Lifecycle management) di StorageGRID determinano la capacità necessaria per memorizzare i backup CommVault e influiscono sul dimensionamento del grid.

La replica ILM di StorageGRID è uno dei due meccanismi utilizzati da StorageGRID per memorizzare i dati

degli oggetti. Quando StorageGRID assegna gli oggetti a una regola ILM che replica i dati, il sistema crea copie esatte dei dati degli oggetti e memorizza le copie nei nodi storage.

Erasure coding è il secondo metodo utilizzato da StorageGRID per memorizzare i dati degli oggetti. Quando StorageGRID assegna gli oggetti a una regola ILM configurata per creare copie con erasure coding, suddivide i dati degli oggetti in frammenti di dati. Calcola quindi ulteriori frammenti di parità e memorizza ogni frammento su un nodo storage diverso. Quando si accede a un oggetto, questo viene riassemblato utilizzando i frammenti memorizzati. Se un frammento di dati o un frammento di parità si danneggia o viene perso, l'algoritmo di erasure coding può ricreare quel frammento utilizzando un sottoinsieme dei dati e dei frammenti di parità rimanenti.

I due meccanismi richiedono diverse quantità di storage, come dimostrano questi esempi:

- Se si memorizzano due copie replicate, il carico di storage raddoppia.
- Se si archivia una copia con erasure coding 2+1, l'overhead dello storage aumenta di 1,5 volte.

Per la soluzione sottoposta a test, è stata utilizzata un'implementazione StorageGRID entry-level su un singolo sito:

- Nodo amministrativo: Macchina virtuale VMware (VM)
- Bilanciamento del carico: VMware VM
- Nodi storage: 4x SG5712 PB con 4TB dischi
- Nodo amministrativo primario e nodo gateway: Macchine virtuali VMware con i requisiti minimi del carico di lavoro di produzione

StorageGRID supporta anche i sistemi di bilanciamento del carico di terze parti.

Di solito, StorageGRID viene implementato in due o più siti con policy di data Protection che replicano i dati per proteggersi dai guasti a livello di nodo e di sito. Effettuando il backup dei dati su StorageGRID, i dati saranno protetti da copie multiple o dall'erasure coding che separa e riassembla i dati in modo affidabile attraverso un algoritmo.

È possibile utilizzare lo strumento di dimensionamento "Fusion" per dimensionare la griglia.

Scalabilità

È possibile espandere un sistema NetApp StorageGRID aggiungendo storage ai nodi storage, aggiungendo nuovi nodi grid a un sito esistente o aggiungendo un nuovo sito per il data center. È possibile eseguire espansioni senza interrompere il funzionamento del sistema corrente.
StorageGRID scala le performance utilizzando nodi con performance più elevate per i nodi storage o l'appliance fisica che esegue il bilanciamento del carico e i nodi amministrativi o semplicemente aggiungendo nodi aggiuntivi.

Per ulteriori informazioni sull'espansione del sistema StorageGRID, vedere "Guida all'espansione di StorageGRID 11,9".

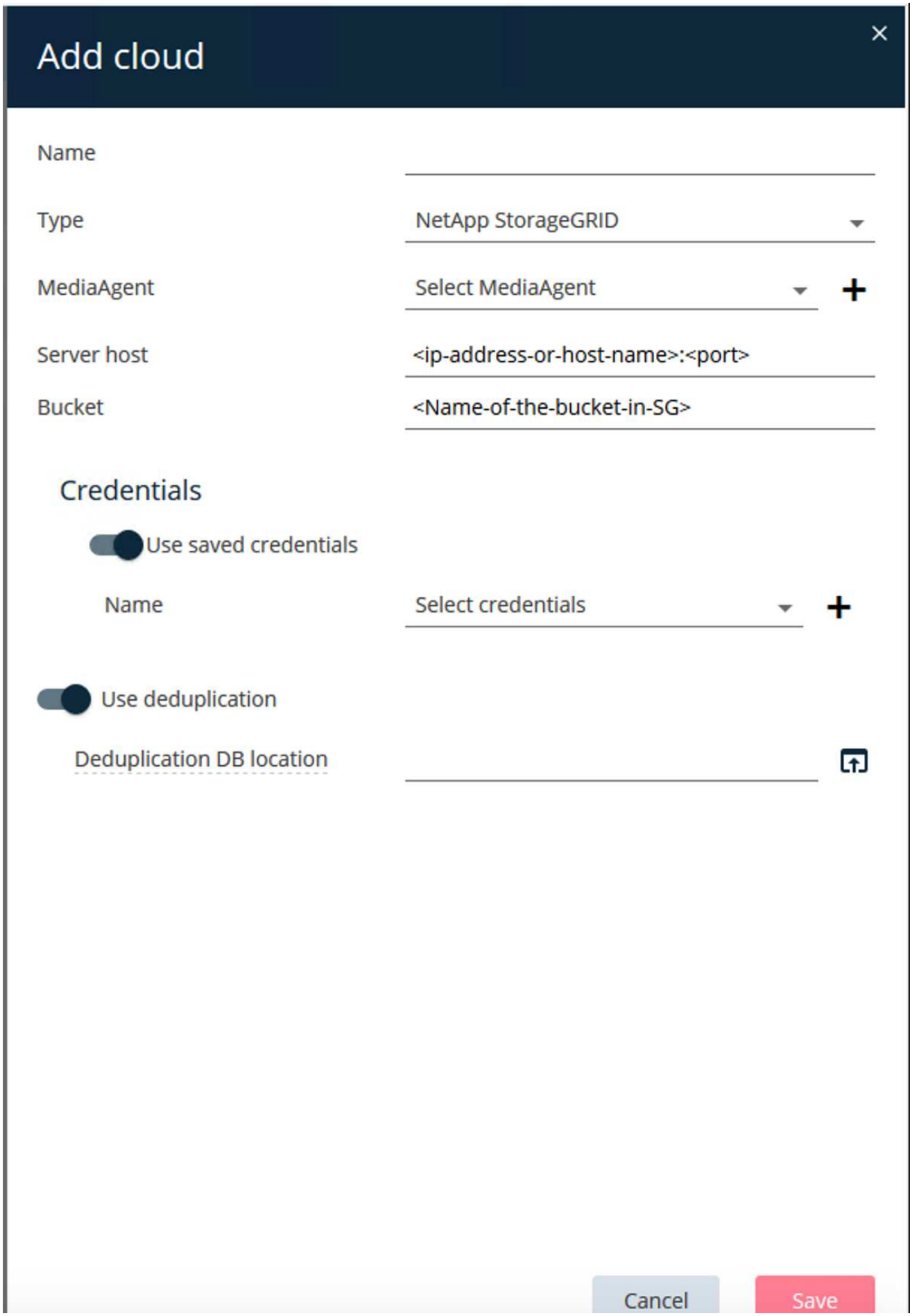
Eseguire un lavoro di protezione dati

Per configurare StorageGRID con CommVault complete Backup and Recovery for NetApp, sono stati eseguiti i seguenti passaggi per aggiungere StorageGRID come libreria cloud all'interno del software CommVault.

Fase 1: Configurare CommVault con StorageGRID

Fasi

1. Effettua l’accesso al CommVault Command Center. Nel pannello di sinistra, fare clic su archiviazione > Cloud > Aggiungi per visualizzare e rispondere alla finestra di dialogo Aggiungi cloud:


Add cloud
Name
Type
NetApp StorageGRID
MediaAgent
Select MediaAgent
Server host
<ip-address-or-host-name>:<port>
Bucket
<Name-of-the-bucket-in-SG>
Credentials
Use saved credentials
Name
Select credentials
Use deduplication
Deduplication DB location
Cancel
Save

2. Per tipo, selezionare NetApp StorageGRID.
3. Per MediaAgent, selezionare tutte le voci associate alla libreria cloud.
4. Per host server, immettere l'indirizzo IP o il nome host dell'endpoint StorageGRID e il numero di porta.

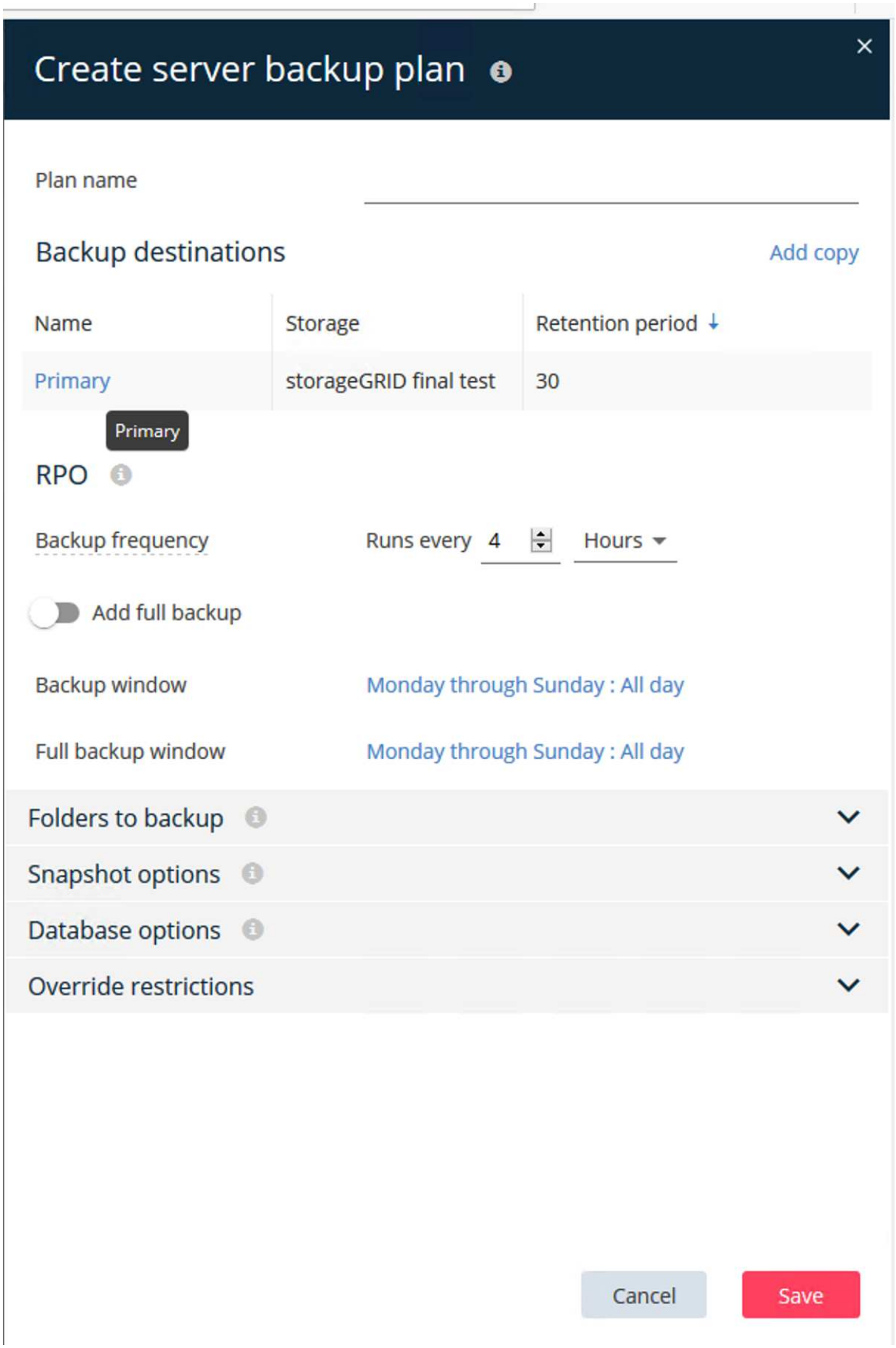
   Seguire le istruzioni riportate nella documentazione di StorageGRID a. "come configurare un endpoint del bilanciamento del carico (porta)". Assicurarsi di disporre di una porta HTTPS con un certificato autofirmato e dell'indirizzo IP o del nome di dominio dell'endpoint StorageGRID.

5. Se si desidera utilizzare la deduplica, attivare questa opzione e specificare il percorso del database di deduplica.
6. Fare clic su Salva.

Fase 2: Creare un piano di backup con StorageGRID come destinazione principale

Fasi

1. Nel pannello di sinistra, selezionare Gestisci > piani per visualizzare e rispondere alla finestra di dialogo Crea piano di backup server.

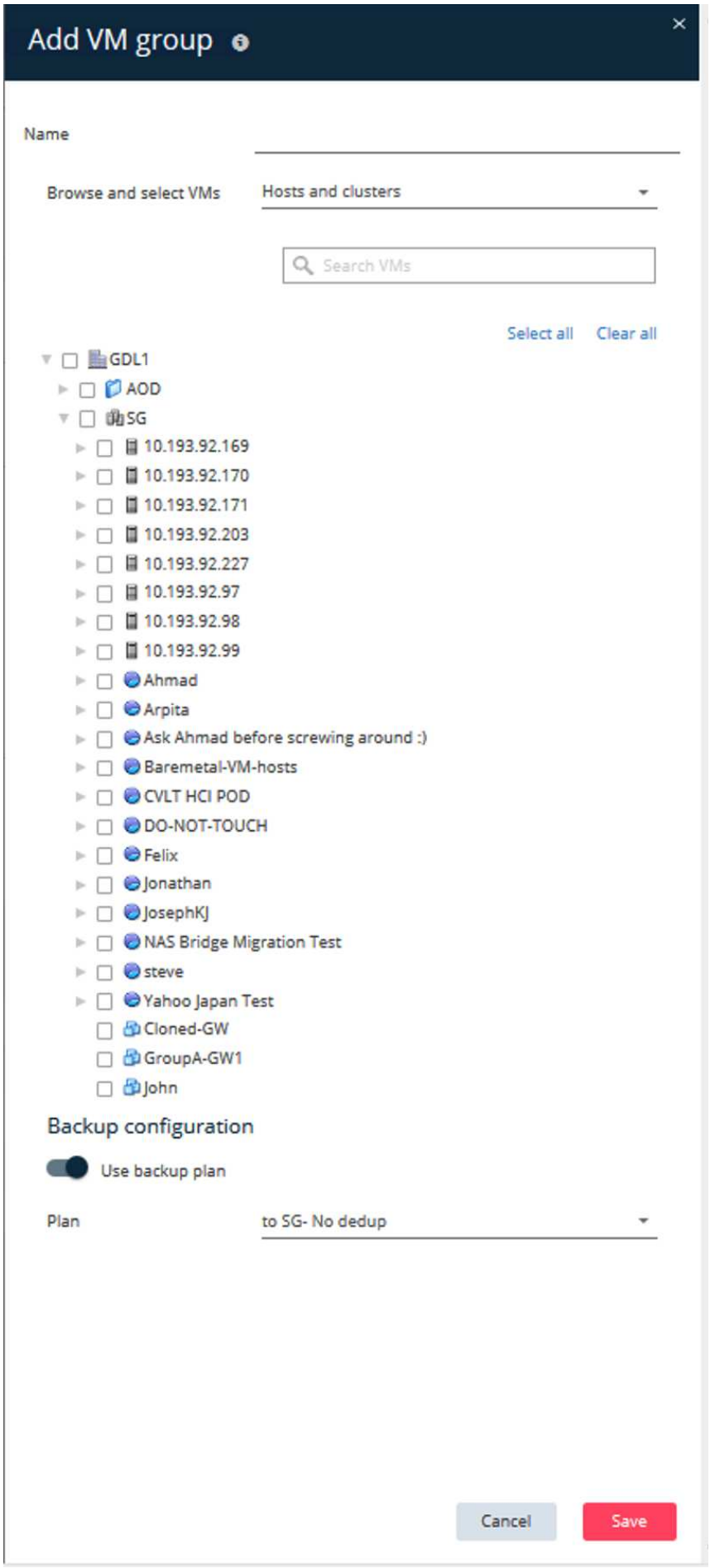

Create server backup plan
Plan name
Backup destinations
Add copy
Name
Storage
Retention period
Primary
storageGRID final test
30
Primary
RPO
Backup frequency
Runs every 4
Hours
Add full backup
Backup window
Monday through Sunday : All day
Full backup window
Monday through Sunday : All day
Folders to backup
Snapshot options
Database options
Override restrictions
Cancel
Save

2. Immettere il nome di un piano.
3. Selezionare la destinazione di backup dello storage di StorageGRID Simple Storage Service (S3) creata in precedenza.
4. Inserisci il periodo di conservazione dei backup e il recovery point objective (RPO) che preferisci.
5. Fare clic su Salva.

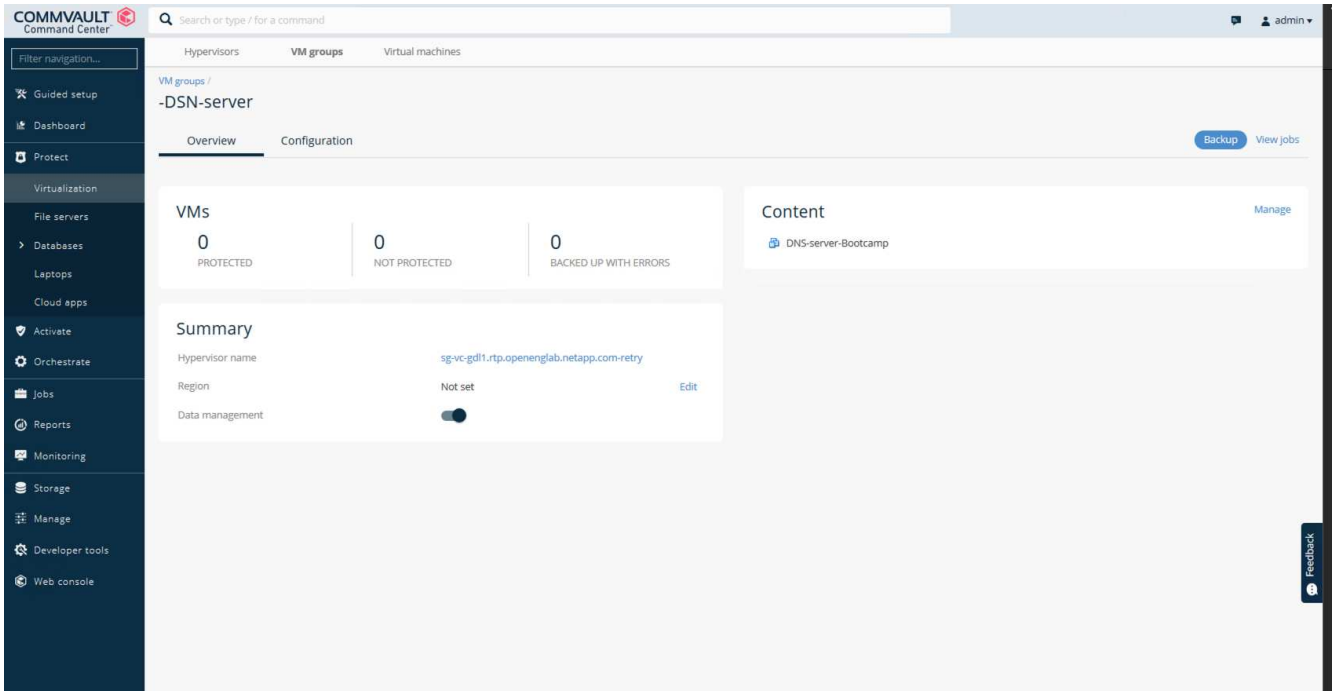
Fase 3: Avviare un processo di backup per proteggere i carichi di lavoro

Fasi

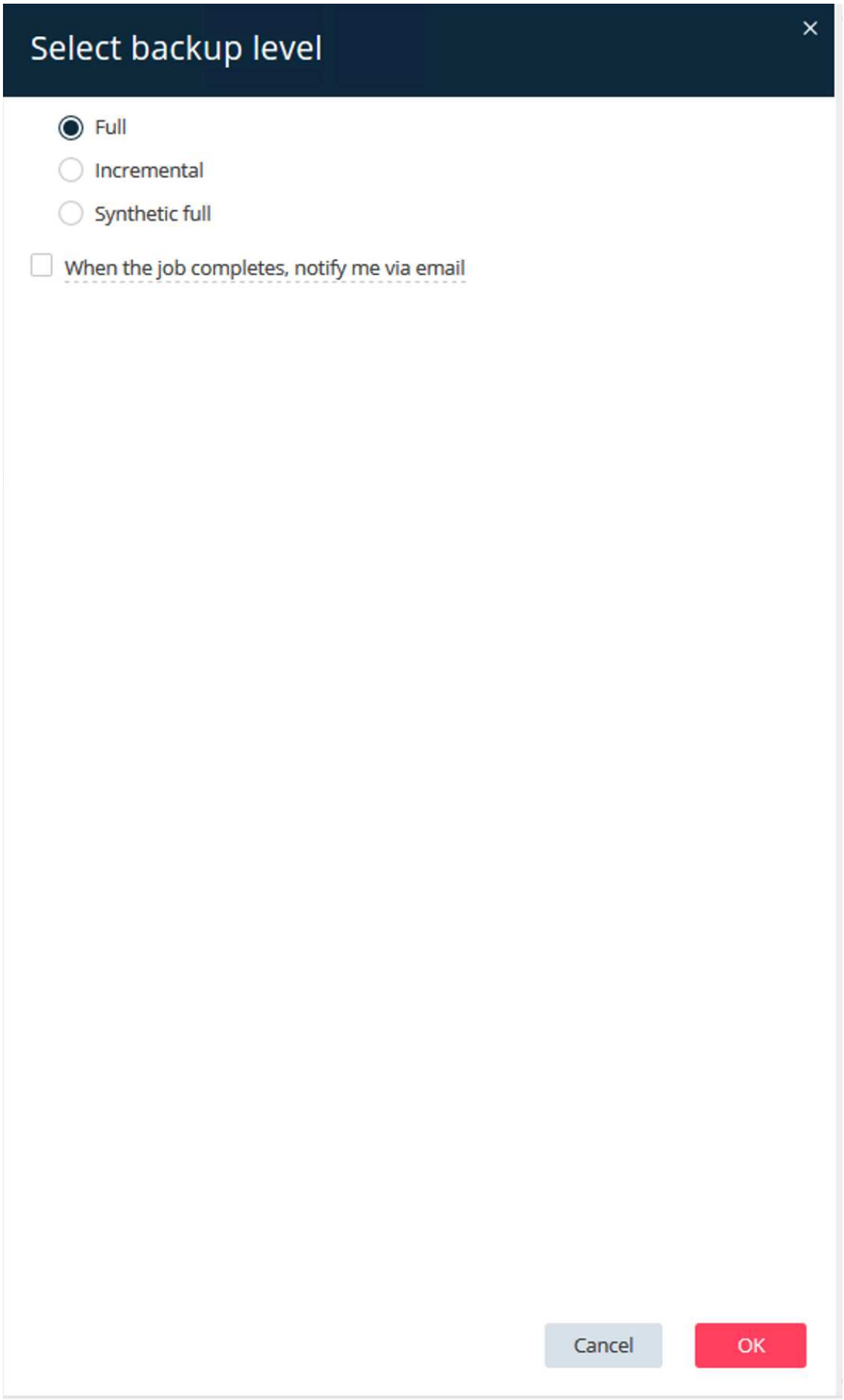
1. Sul CommVault Command Center, selezionare Protect > Virtualization (protezione > virtualizzazione).
2. Aggiunta di un hypervisor VMware vCenter Server.
3. Fare clic sull'hypervisor appena aggiunto.
4. Fare clic su Add VM group (Aggiungi gruppo VM) per rispondere alla finestra di dialogo Add VM Group (Aggiungi gruppo VM) in modo da visualizzare l'ambiente vCenter che si intende proteggere.


Add VM group
Name
Browse and select VMs
Hosts and clusters
Search VMs
Select all
Clear all
GDL1
AOD
SG
10.193.92.169
10.193.92.170
10.193.92.171
10.193.92.203
10.193.92.227
10.193.92.97
10.193.92.98
10.193.92.99
Ahmad
Arpita
Ask Ahmad before screwing around :)
Baremetal-VM-hosts
CVLT HCI POD
DO-NOT-TOUCH
Felix
Jonathan
JosephKJ
NAS Bridge Migration Test
steve
Yahoo Japan Test
Cloned-GW
GroupA-GW1
John
Backup configuration
Use backup plan
Plan
to SG- No dedup
Cancel
Save

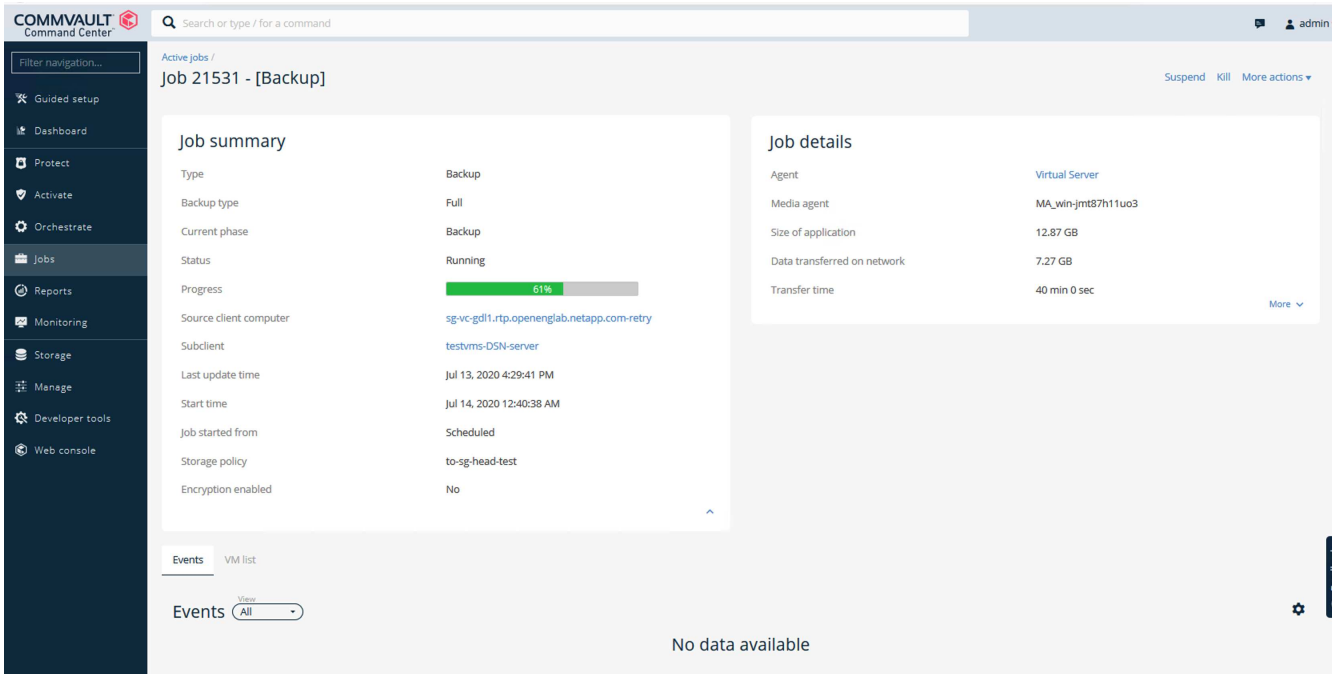
5. Seleziona un datastore, una macchina virtuale o una raccolta di macchine virtuali e inserisci un nome per questo.
6. Selezionare il piano di backup creato nell'attività precedente.
7. Fare clic su Salva per visualizzare il gruppo VM creato.
8. Nell'angolo superiore destro della finestra del gruppo VM, selezionare Backup:



9. Selezionare Full come livello di backup, (facoltativamente) richiedere un'e-mail al termine del backup, quindi fare clic su OK per avviare il processo di backup:


Select backup level
Full
Incremental
Synthetic full
When the job completes, notify me via email
Cancel
OK

10. Passare alla pagina di riepilogo dei lavori per visualizzare le metriche dei lavori:



Esaminare i test delle prestazioni di base

Nell'operazione di copia ausiliaria, quattro CommVault MediaAgent hanno eseguito il backup dei dati su un sistema NetApp AFF A300 e una copia ausiliaria è stata creata su NetApp StorageGRID. Per informazioni dettagliate sull'ambiente di configurazione dei test, leggere la sezione progettazione della soluzione e Best practice nel "Data Protection scale-out NetApp con CommVault" report tecnico.

I test sono stati eseguiti con 100 VM e 1000 VM, entrambi con una combinazione di 50/50 VM Windows e CentOS. La tabella seguente mostra i risultati dei nostri test di base sulle prestazioni:

Operazione	Velocità di backup	Ripristina velocità
Copia AUX	2 TB/ora	1,27 TB/ora
Diretto da e verso l'oggetto (deduplica attivata)	2,2 TB/ora	1,22 TB/ora

Per testare le performance di vecchiaia, sono stati eliminati 2,5 milioni di oggetti. Come mostrato nelle Figure 2 e 3, l'esecuzione di eliminazione è stata completata in meno di 3 ore e ha liberato più di 80TB GB di spazio. La seriografia di eliminazione è iniziata alle 10:30:00 AM.

Figura 1: Eliminazione di 2,5 milioni (80TB) oggetti in meno di 3 ore.

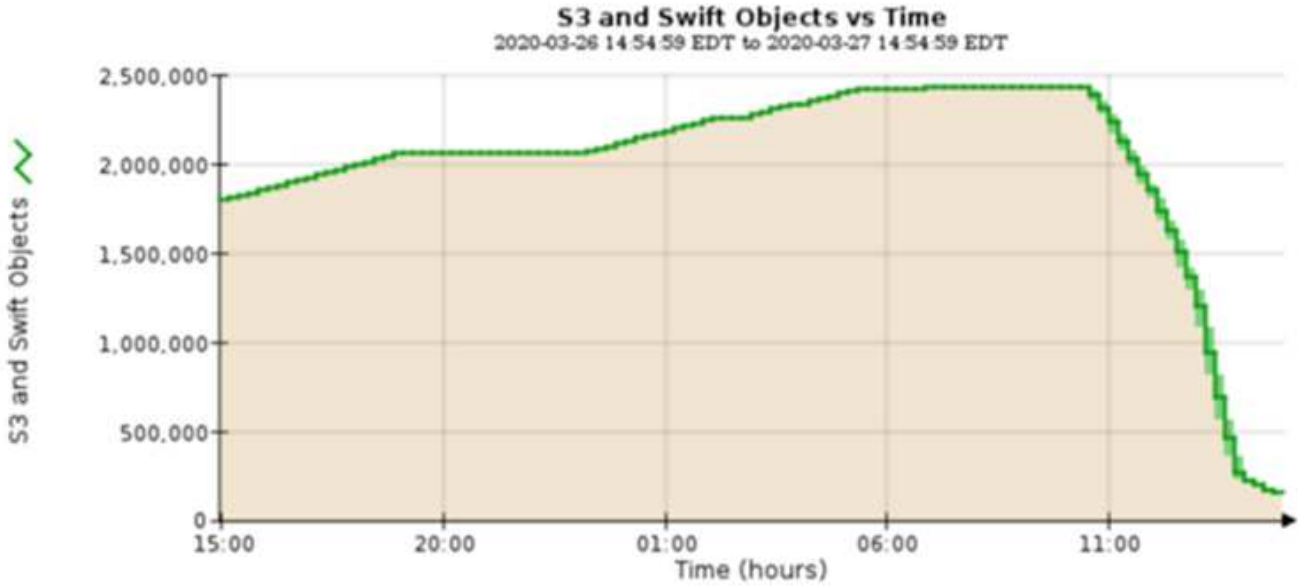
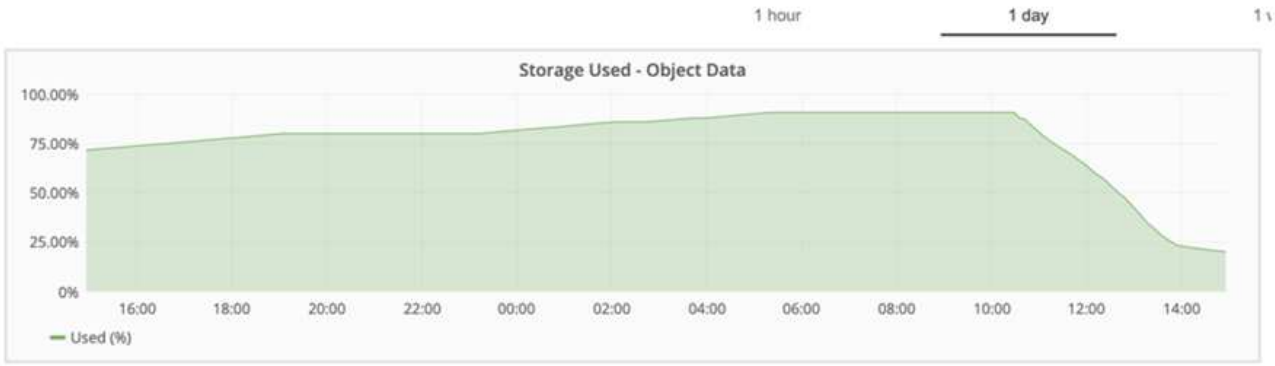


Figura 2: Liberare 80TB TB di storage in meno di 3 ore.



Suggerimento del livello di coerenza della benna

NetApp StorageGRID consente all'utente finale di selezionare il livello di coerenza per le operazioni eseguite sugli oggetti nei bucket Simple Storage Service (S3).

CommVault MediaAgent è il data mover di un ambiente CommVault. Nella maggior parte dei casi, i MediaAgent sono configurati per scrivere localmente in un sito StorageGRID primario. Per questo motivo, si consiglia un elevato livello di coerenza all'interno di un sito primario locale. Utilizza le seguenti linee guida quando imposti il livello di coerenza sui bucket CommVault creati in StorageGRID.

Se si dispone di una versione di CommVault precedente alla 11.0.0 - Service Pack 16, valutare la possibilità di aggiornare CommVault alla versione più recente. Se questa opzione non è disponibile, attenersi alle linee guida per la versione in uso.

- Versioni di CommVault precedenti alla 11.0.0 - Service Pack 16.* nelle versioni precedenti alla 11.0.0 - Service Pack 16, CommVault esegue S3 TESTE e OTTIENE le operazioni su oggetti inesistenti come parte del processo di ripristino e pruning. Impostare il livello di coerenza del bucket su un sito sicuro per ottenere un livello di coerenza ottimale per i backup CommVault su StorageGRID.
- CommVault versioni 11.0.0 - Service Pack 16 e successive.* nelle versioni 11.0.0 - Service Pack 16 e successive, il numero di operazioni HEAD S3 e GET eseguite su oggetti inesistenti viene ridotto al minimo.

Impostare il livello di coerenza del bucket predefinito su Read-after-new-write per garantire un elevato livello di coerenza nell'ambiente CommVault e StorageGRID.

TR-4626: Bilanciatori del carico

Utilizza sistemi di bilanciamento del carico di terze parti con StorageGRID

Scopri il ruolo di bilanciatori del carico globale e di terze parti in sistemi storage a oggetti come StorageGRID.

Indicazioni generali per l'implementazione di NetApp® StorageGRID® con sistemi di bilanciamento del carico di terze parti.

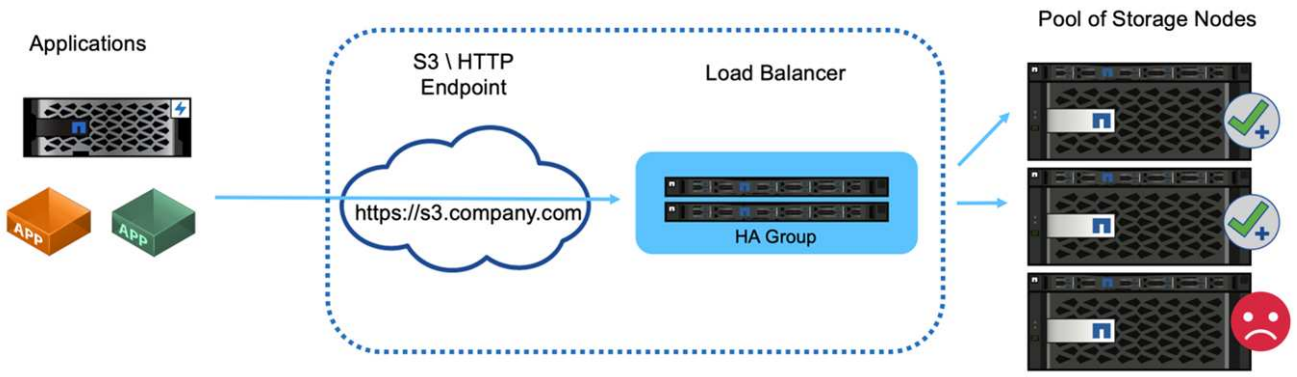
Lo storage a oggetti è sinonimo del termine cloud storage e, come ti aspetti, le applicazioni che sfruttano il cloud storage indirizzano tale storage attraverso un URL. Dietro questo semplice URL, StorageGRID può scalare capacità, performance e durata in un singolo sito o in siti distribuiti geograficamente. Il componente che rende possibile questa semplicità è il bilanciamento del carico.

Lo scopo di questo documento è informare i clienti StorageGRID sulle opzioni del bilanciamento del carico e fornire una guida generale per la configurazione dei bilanciatori del carico di terze parti.

Nozioni di base sul bilanciamento del carico

I bilanciatori del carico sono un componente essenziale di un sistema storage a oggetti di livello Enterprise come StorageGRID. StorageGRID è composto da più nodi storage, ciascuno dei quali può presentare l'intero spazio dei nomi di Simple Storage Service (S3) per una determinata istanza di StorageGRID. I bilanciatori del carico creano un endpoint altamente disponibile dietro cui è possibile posizionare i nodi StorageGRID. StorageGRID è un'esclusiva tra i sistemi di storage a oggetti compatibili con S3, in quanto offre un proprio bilanciamento del carico, ma supporta anche bilanciatori del carico di terze parti o General-purpose come F5, Citrix Netscaler, ha Proxy, NGINX e così via.

Nella figura seguente viene utilizzato l'URL di esempio/nome di dominio completo (FQDN) "s3.company.com". Il bilanciamento del carico crea un IP virtuale (VIP) che viene risolto all'FQDN tramite DNS, quindi indirizza le richieste dalle applicazioni a un pool di nodi StorageGRID. Il bilanciamento del carico esegue un controllo dello stato di salute su ogni nodo e stabilisce solo connessioni a nodi sani.



La figura mostra il bilanciamento del carico fornito da StorageGRID, ma il concetto è lo stesso per i bilanciatori del carico di terze parti. Le applicazioni stabiliscono una sessione HTTP utilizzando il VIP sul bilanciamento del carico e il traffico passa attraverso il bilanciamento del carico fino ai nodi di storage. Per impostazione predefinita, tutto il traffico, dall'applicazione al bilanciamento del carico e dal bilanciamento del carico al nodo storage è crittografato tramite HTTPS. HTTP è un'opzione supportata.

Bilanciatori del carico locali e globali

Esistono due tipi di bilanciatori del carico:

- **Gestione del traffico locale (LTM)**. Distribuisce le connessioni su un pool di nodi in un singolo sito.
- **Bilanciamento del carico di servizio globale (GSLB)**. Distribuisce le connessioni su siti multipli, bilanciando efficacemente il carico LTM. Pensate a un GSLB come a un server DNS intelligente. Quando un client richiede un URL endpoint StorageGRID, il GSLB lo risolve al VIP di un LTM in base alla disponibilità o ad altri fattori (ad esempio, quale sito può fornire una latenza inferiore all'applicazione). Mentre un LTM è sempre richiesto, un GSLB è opzionale a seconda del numero di siti StorageGRID e dei requisiti dell'applicazione.

Dove trovare ulteriori informazioni

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

- Centro di documentazione NetApp StorageGRIDhttps://docs.netapp.com/us-en/storagegrid/[]
- Abilitazione NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Considerazioni sulla progettazione del bilanciamento del carico StorageGRID F5 https://www.netapp.com/blog/storagegrid-f5-load-balancer-design-considerations/
- Loadbalancer.org—Load bilanciamento NetApp StorageGRID https://www.loadbalancer.org/applications/load-balancing-netapp-storagegrid/
- Kemp - NetApp StorageGRID di bilanciamento del carico https://support.kemptechnologies.com/hc/en-us/articles/360045186451-NetApp-StorageGRID

Utilizzare i bilanciatori di carico StorageGRID

Scopri il ruolo di un bilanciatore del carico StorageGRID Gateway Node.

Linee guida generali per l'implementazione dei nodi gateway NetApp® StorageGRID®.

Bilanciamento del carico del nodo gateway StorageGRID rispetto a quello di terze parti

StorageGRID è un'esclusiva tra i vendor di storage a oggetti compatibili con S3, in quanto offre un bilanciatore del carico nativo disponibile come appliance, VM o container costruiti ad hoc. Il bilanciamento del carico fornito da StorageGRID è anche detto nodo gateway.

Per i clienti che non dispongono già di un sistema di bilanciamento del carico, ad esempio F5, Citrix e così via, l'implementazione di un sistema di bilanciamento del carico di terze parti può rivelarsi molto complessa. Il bilanciamento del carico StorageGRID semplifica notevolmente le operazioni di bilanciamento del carico.

Il Gateway Node è un bilanciatore del carico di livello Enterprise, altamente disponibile e dalle performance elevate. I clienti possono scegliere di implementare il nodo gateway, il sistema di bilanciamento del carico di terze parti o anche entrambi nello stesso grid. Il nodo gateway è un gestore del traffico locale rispetto a un GSLB.

Il bilanciamento del carico StorageGRID offre i seguenti vantaggi:

- **Semplicità**. Configurazione automatica di pool di risorse, controlli dello stato di salute, applicazione di patch e manutenzione, il tutto gestito da StorageGRID.
- **Prestazione**. Il bilanciatore del carico StorageGRID è dedicato a StorageGRID, può fornire caching ad alte

prestazioni e non compete con altre applicazioni per la larghezza di banda.

- **Costo**. Le versioni di macchina virtuale (VM) e container sono fornite senza costi aggiuntivi.
- **Classificazioni del traffico**. La funzionalità Advanced Traffic Classification consente di applicare regole QoS specifiche di StorageGRID insieme all'analisi dei workload.
- **Caratteristiche specifiche future di StorageGRID**. StorageGRID continuerà a ottimizzare e aggiungere funzioni innovative al bilanciatore di carico nelle prossime release.

In quanto nodo integrato di StorageGRID, il gestore del traffico locale ha la possibilità di utilizzare un controllo avanzato dello stato per distribuire le richieste in base allo stato di integrità, al carico e alla disponibilità delle risorse del nodo di archiviazione. Inoltre, ha la capacità di distribuire il carico su più siti quando i costi del collegamento StorageGRID sono impostati su "0" tra i siti. Nel caso in cui i nodi di archiviazione non siano disponibili ma il nodo gateway sia disponibile in un sito, il carico verrà automaticamente indirizzato a un altro sito nella rete.

La funzionalità di memorizzazione nella cache del bilanciatore del carico del Gateway Node è pensata per fornire un miglioramento sostanziale delle prestazioni per determinati carichi di lavoro (ad esempio la formazione dell'intelligenza artificiale) che rileggono un set di dati più volte durante l'elaborazione di tali dati. I nodi gateway di memorizzazione nella cache possono anche essere distribuiti fisicamente distanti dal resto della griglia, consentendo prestazioni migliori e un minore utilizzo della rete WAN in alcuni carichi di lavoro. La cache funziona in modalità di lettura in cui le scritture non vengono memorizzate nella cache e non modificano lo stato della cache. Ogni nodo del gateway di memorizzazione nella cache funziona indipendentemente da qualsiasi altro nodo del gateway di memorizzazione nella cache.

Per i dettagli sulla distribuzione del nodo gateway StorageGRID , vedere "Documentazione StorageGRID" .

Informazioni su come implementare i certificati SSL per HTTPS in StorageGRID

Comprendere l'importanza e i passaggi per implementare i certificati SSL in StorageGRID.

Se si utilizza HTTPS, è necessario disporre di un certificato SSL (Secure Sockets Layer). Il protocollo SSL identifica i client e gli endpoint, convalidandoli come attendibili. SSL fornisce anche la crittografia del traffico. Il certificato SSL deve essere attendibile dai client. A tal fine, il certificato SSL può provenire da un'autorità di certificazione (CA) globalmente attendibile, ad esempio DigiCert, una CA privata in esecuzione nell'infrastruttura o un certificato autofirmato generato dall'host.

L'utilizzo di un certificato CA globale attendibile è il metodo preferito poiché non sono necessarie ulteriori azioni sul lato client. Il certificato viene caricato nel bilanciamento del carico o StorageGRID e i client si fidano e si connettono all'endpoint.

L'utilizzo di una CA privata richiede l'aggiunta al client di tutti i certificati subordinati e della directory principale. Il processo per considerare attendibile un certificato CA privato può variare in base al sistema operativo e alle applicazioni del client. Ad esempio, in ONTAP per FabricPool, è necessario caricare ciascun certificato nella catena individualmente (certificato di origine, certificato di subordinazione, certificato di endpoint) nel cluster ONTAP.

L'utilizzo di un certificato autofirmato richiede al client di considerare attendibile il certificato fornito senza alcuna CA per verificarne l'autenticità. Alcune applicazioni potrebbero non accettare certificati autofirmati e non essere in grado di ignorare la verifica.

Il posizionamento del certificato SSL nel percorso StorageGRID di bilanciamento del carico del client dipende da dove è necessaria la terminazione SSL. È possibile configurare un bilanciamento del carico come endpoint di terminazione per il client, quindi eseguire nuovamente la crittografia o la crittografia a caldo con un nuovo

certificato SSL per il bilanciamento del carico alla connessione StorageGRID. In alternativa, è possibile passare attraverso il traffico e lasciare che StorageGRID sia l'endpoint di terminazione SSL. Se il bilanciamento del carico è l'endpoint di terminazione SSL, il certificato viene installato sul bilanciamento del carico e contiene il nome del soggetto per il nome/URL DNS e qualsiasi nome URL/DNS alternativo per il quale un client è configurato per connettersi alla destinazione StorageGRID tramite il bilanciamento del carico, inclusi i nomi dei caratteri jolly. Se il bilanciamento del carico è configurato per il pass-through, il certificato SSL deve essere installato in StorageGRID. Anche in questo caso, il certificato deve contenere il nome del soggetto per il nome/URL DNS e tutti i nomi URL/DNS alternativi per i quali un client è configurato per connettersi alla destinazione StorageGRID tramite il sistema di bilanciamento del carico, inclusi i nomi di caratteri jolly. Non è necessario includere nel certificato i nomi dei singoli nodi di archiviazione, ma solo gli URL degli endpoint.

Configurare il bilanciamento del carico di terze parti attendibile in StorageGRID

Scopri come configurare il bilanciamento del carico di terze parti attendibile in StorageGRID.

Se si utilizzano uno o più bilanciatori di carico Layer 7 esterni e un bucket S3 o policy di gruppo basati su IP, StorageGRID deve determinare l'indirizzo IP reale del mittente. Ciò avviene guardando l'intestazione X-Forwarding-for (XFF), che viene inserita nella richiesta dal bilanciatore di carico. Poiché l'intestazione XFF può essere facilmente sottoposta a spoofing nelle richieste inviate direttamente ai nodi di archiviazione, StorageGRID deve confermare che ogni richiesta è stata instradata da un bilanciatore di carico di livello 7 attendibile. Se StorageGRID non è in grado di considerare attendibile l'origine della richiesta, ignorerà l'intestazione XFF. È disponibile un'API di gestione griglia che consente di configurare un elenco di bilanciatori del carico di livello 7 esterni attendibili. Questa nuova API è privata ed è soggetta a modifiche nelle versioni future di StorageGRID. Per le informazioni più aggiornate, vedere l'articolo della Knowledge base, "Come configurare StorageGRID per il funzionamento con sistemi di bilanciamento del carico Layer 7 di terze parti".

Informazioni sui bilanciatori del carico dei gestori del traffico locali

Esplora le linee guida per i bilanciatori del carico del gestore del traffico locale e determina la configurazione ottimale.

Quanto segue viene presentato come guida generale per la configurazione dei sistemi di bilanciamento del carico di terze parti. Collabora con l'amministratore del sistema di bilanciamento del carico per determinare la configurazione ottimale per il tuo ambiente.

Creare un gruppo di risorse di nodi di archiviazione

Raggruppare i nodi di storage StorageGRID in un pool di risorse o in un gruppo di servizi (la terminologia potrebbe differire con specifici bilanciatori del carico). I nodi storage StorageGRID presentano l'API S3 sulle seguenti porte:

- S3 HTTPS: 18082
- S3 HTTP: 18084

La maggior parte dei clienti sceglie di presentare le API sul server virtuale tramite le porte HTTPS e HTTP standard (443 e 80).

> Ogni sito StorageGRID richiede un'impostazione predefinita di tre nodi storage, due dei quali devono essere integri.

Controllo dello stato di salute

I sistemi di bilanciamento del carico di terze parti richiedono un metodo per determinare lo stato di salute di ogni nodo e la sua idoneità a ricevere il traffico. NetApp consiglia di utilizzare il metodo HTTP `OPTIONS` per eseguire il controllo dello stato di salute. Il bilanciamento del carico invia richieste HTTP `OPTIONS` a ogni singolo nodo di storage e prevede una `200` risposta di stato.

Se un nodo di archiviazione non fornisce una `200` risposta, tale nodo non è in grado di eseguire il servizio delle richieste di archiviazione. I requisiti dell'applicazione e dell'azienda devono determinare il timeout per questi controlli e l'azione intrapresa dal bilanciamento del carico.

Ad esempio, se tre dei quattro nodi storage del data center 1 non sono attivi, è possibile indirizzare tutto il traffico al data center 2.

L'intervallo di polling consigliato è una volta al secondo, contrassegnando il nodo offline dopo tre controlli non riusciti.

Esempio di controllo dello stato di salute di S3

Nell'esempio seguente, inviamo `OPTIONS` e controlliamo `200 OK`. Lo utilizziamo `OPTIONS` perché Amazon S3) non supporta richieste non autorizzate.

```
curl -X OPTIONS https://10.63.174.75:18082 --verbose --insecure
* Rebuilt URL to: https://10.63.174.75:18082/
*   Trying 10.63.174.75...
* TCP_NODELAY set
* Connected to 10.63.174.75 (10.63.174.75) port 18082 (#0)
* TLS 1.2 connection using TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* Server certificate: webscale.stl.netapp.com
* Server certificate: NetApp Corp Issuing CA 1
* Server certificate: NetApp Corp Root CA
> OPTIONS / HTTP/1.1
> Host: 10.63.174.75:18082
> User-Agent: curl/7.51.0
> Accept: /
>
< HTTP/1.1 200 OK
< Date: Mon, 22 May 2017 15:17:30 GMT
< Connection: KEEP-ALIVE
< Server: StorageGRID/10.4.0
< x-amz-request-id: 3023514741
```

Controlli dello stato di salute basati su file o contenuti

In generale, NetApp non consiglia controlli dello stato di salute basati su file. In genere, un file di piccole dimensioni —`healthcheck.htm`, ad esempio, viene creato in un bucket con un criterio di sola lettura. Questo file viene quindi recuperato e valutato dal bilanciamento del carico. Questo approccio presenta diversi svantaggi:

- **Dipendente da un unico conto.** Se l'account proprietario del file è disattivato, il controllo di integrità non riesce e non vengono elaborate richieste di archiviazione.
- **Regole per la protezione dei dati.** Lo schema di protezione dei dati predefinito è un approccio a due copie. In questo scenario, se i due nodi storage che ospitano il file di controllo dello stato di salute non sono disponibili, il controllo dello stato di salute non riesce e le richieste di storage non vengono inviate ai nodi storage sani, rendendo la griglia offline.
- **Registro di controllo bloat.** Il bilanciamento del carico recupera il file da ogni nodo storage ogni X minuti, creando molte voci di registro di controllo.
- **Uso intensivo delle risorse.** Il recupero del file di controllo dello stato da ogni nodo ogni pochi secondi consuma le risorse della rete e della griglia.

Se è necessario un controllo dello stato di salute basato sul contenuto, utilizzare un tenant dedicato con un bucket S3 dedicato.

Persistenza della sessione

La persistenza della sessione, o stickiness, si riferisce al tempo in cui una data sessione HTTP può persistere. Per impostazione predefinita, le sessioni vengono interrotte dai nodi storage dopo 10 minuti. Una persistenza più lunga può portare a performance migliori, perché le applicazioni non devono ristabilire le sessioni per ogni azione; tuttavia, mantenendo queste sessioni aperte si consumano le risorse. Se ritieni che il tuo carico di lavoro trarrà beneficio, puoi ridurre la persistenza della sessione su un bilanciamento del carico di terze parti.

Indirizzamento virtuale in stile host

Lo stile in hosting virtuale è ora il metodo predefinito per AWS S3 e, sebbene StorageGRID e molte applicazioni supportino ancora lo stile del percorso, è consigliabile implementare il supporto in stile in hosting virtuale. Le richieste in stile host virtuale hanno il bucket come parte del nome host.

Per supportare lo stile host virtuale, procedere come segue:

- Supporta ricerche DNS con caratteri jolly: *.s3.company.com
- Utilizzare un certificato SSL con nomi alt del soggetto per supportare i caratteri jolly: *.s3.company.com alcuni clienti hanno espresso preoccupazioni per la sicurezza riguardo all'uso dei certificati jolly. StorageGRID continua a supportare l'accesso in stile percorso, così come le applicazioni chiave come FabricPool. Detto questo, alcune chiamate API S3 non riescono o si comportano in modo errato senza supporto di hosting virtuale.

Terminazione SSL

La terminazione SSL dei sistemi di bilanciamento del carico di terze parti offre vantaggi in termini di sicurezza. Se il bilanciamento del carico è compromesso, la griglia viene suddivisa in comparti.

Sono disponibili tre configurazioni supportate:

- **Pass-through SSL.** Il certificato SSL viene installato su StorageGRID come certificato server personalizzato.
- **Terminazione SSL e nuova crittografia (consigliata).** Ciò potrebbe essere utile se si sta già eseguendo la gestione dei certificati SSL sul sistema di bilanciamento del carico piuttosto che installare il certificato SSL su StorageGRID. Questa configurazione offre un ulteriore vantaggio in termini di sicurezza nel limitare la superficie di attacco al bilanciatore del carico.
- **Terminazione SSL con HTTP.** In questa configurazione, SSL viene terminato sul bilanciamento del carico di terze parti e la comunicazione dal bilanciamento del carico a StorageGRID non è crittografata per sfruttare il off-load SSL (con librerie SSL incorporate nei processori moderni questo è di limitato beneficio).

Configurazione pass-through

Se si preferisce configurare il bilanciamento del carico per il pass-through, è necessario installare il certificato su StorageGRID. Andare al **Configurazione › certificati server › certificato server endpoint del servizio API di archiviazione oggetti**.

Visibilità IP del client di origine

StorageGRID 11,4 ha introdotto il concetto di un sistema di bilanciamento del carico di terze parti affidabile. Per inoltrare l'IP dell'applicazione client a StorageGRID, è necessario configurare questa funzione. Per ulteriori informazioni, vedere "Come configurare StorageGRID per il funzionamento con sistemi di bilanciamento del carico Layer 7 di terze parti."

Per abilitare l'intestazione XFF per la visualizzazione dell'IP dell'applicazione client, attenersi alla seguente procedura:

Fasi

1. Registrare l'IP del client nel registro di controllo.
2. Utilizzare `aws:SourceIp` criteri di gruppo o bucket S3.

Strategie di bilanciamento del carico

La maggior parte delle soluzioni di bilanciamento del carico offre molteplici strategie per il bilanciamento del carico. Le seguenti sono strategie comuni:

- **Rotondi.** Un adattamento universale ma soffre di pochi nodi e grandi trasferimenti che ostruiscono i singoli nodi.
- **Connessione minima.** Ideale per workload di oggetti piccoli e misti, con una distribuzione equa delle connessioni a tutti i nodi.

La scelta dell'algoritmo diventa meno importante con un numero crescente di nodi storage tra cui scegliere.

Percorso dei dati

Tutti i flussi di dati attraverso i bilanciatori del carico del gestore del traffico locale. StorageGRID non supporta il routing diretto del server (DSR).

Verifica della distribuzione dei collegamenti

Per verificare che il metodo in uso distribuisca il carico in modo uniforme tra i nodi storage, controllare le sessioni stabilite su ciascun nodo in un determinato sito:

- **Metodo UI.** Andare al **supporto › metriche › Panoramica S3 › sessioni HTTP LDR**
- **API metriche.** Uso `storagegrid_http_sessions_incoming_currently_established`

Scopri i pochi casi di utilizzo per le configurazioni StorageGRID

Scopri alcuni casi di utilizzo per le configurazioni StorageGRID implementate dai clienti e da NetApp IT.

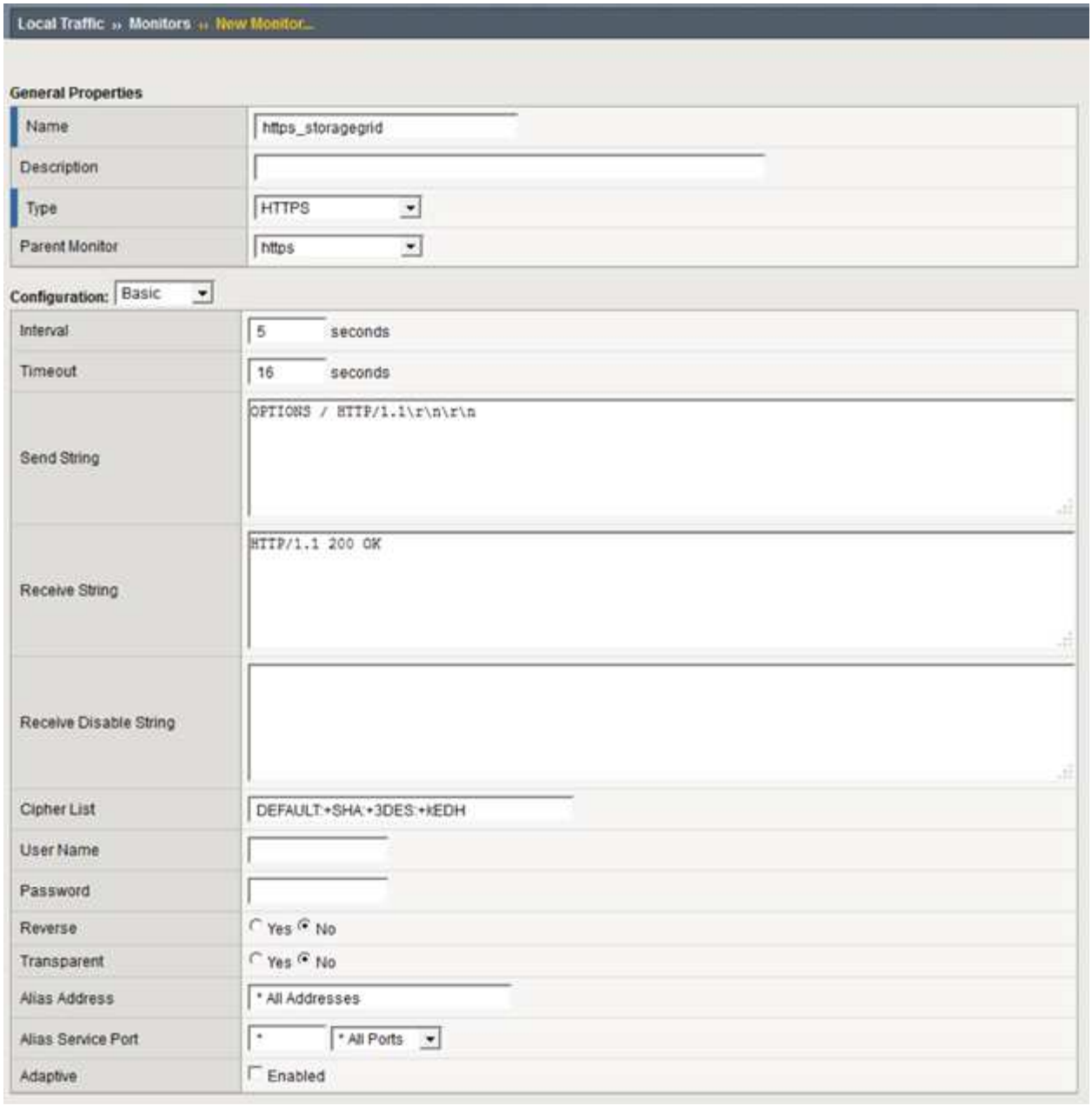
I seguenti esempi illustrano le configurazioni implementate dai clienti StorageGRID, incluso NetApp IT.

F5 BIG-IP, il monitor di controllo dello stato del gestore del traffico locale per bucket S3

Per configurare il monitor di controllo dello stato del gestore del traffico locale BIG-IP F5, attenersi alla seguente procedura:

Fasi

1. Creare un nuovo monitor.
   a. Nel campo tipo, immettere `HTTPS`.
   b. Configurare l'intervallo e il timeout come desiderato.
   c. Nel campo Invia stringa, immettere `OPTIONS / HTTP/1.1\r\n\r\n.` \r\n sono ritorni a capo; versioni diverse del software BIG-IP richiedono zero, uno o due set di sequenze \r\n. Per ulteriori informazioni, vedere https://support.f5.com/csp/article/K10655.
   d. Nel campo Receive String (stringa di ricezione), immettere: `HTTP/1.1 200 OK`.



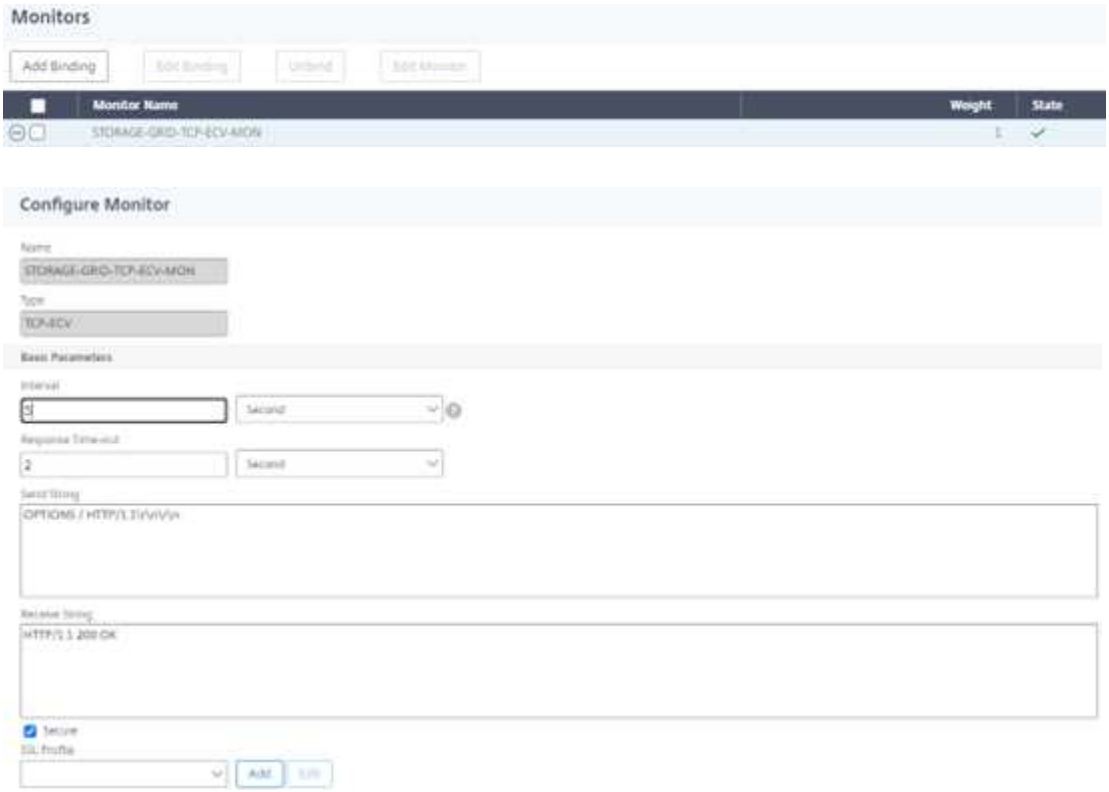
2. In Create Pool (Crea pool) creare un pool per ciascuna porta richiesta.
   a. Assegnare il monitor dello stato creato nel passaggio precedente.
   b. Selezionare un metodo di bilanciamento del carico.
   c. Selezionare la porta di servizio: 18082 (S3).
   d. Aggiungere nodi.

Citrix NetScaler

Citrix NetScaler crea un server virtuale per l'endpoint di storage e fa riferimento ai nodi storage StorageGRID come server applicazioni, che vengono quindi raggruppati in servizi.

Utilizzare il monitor di controllo dello stato HTTPS-ECV per creare un monitor personalizzato per eseguire il controllo dello stato consigliato utilizzando le OPZIONI richiesta e ricezione `200`. HTTP-ECV è configurato con una stringa di invio e convalida una stringa di ricezione.

Per ulteriori informazioni, consultare la documentazione Citrix, "Configurazione di esempio per il monitor di controllo dello stato HTTP-ECV".



Loadbalancer.org

Loadbalancer.org ha eseguito i propri test di integrazione con StorageGRID e dispone di una guida completa alla configurazione: https://pdfs.loadbalancer.org/NetApp_StorageGRID_Deployment_Guide.pdf.

Kemp

Kemp ha condotto i propri test di integrazione con StorageGRID e dispone di una guida alla configurazione completa: https://kemptechnologies.com/solutions/netapp/.

HAProxy

Configurare HAProxy per utilizzare la richiesta di OPZIONI e controllare una risposta di stato 200 per il controllo dello stato in hproxy.cfg. È possibile modificare la porta di binding nella parte anteriore in una porta diversa, ad esempio 443.

Di seguito è riportato un esempio di terminazione SSL su HAProxy:

```
frontend s3
       bind *:443 crt /etc/ssl/server.pem ssl
       default_backend s3-serve
rs
backend s3-servers
       balance leastconn
       option httpchk
       http-check expect status 200
       server dc1-s1 10.63.174.71:18082 ssl verify none check inter 3000
       server dc1-s2 10.63.174.72:18082 ssl verify none check inter 3000
       server dc1-s3 10.63.174.73:18082 ssl verify none check inter 3000
```

Di seguito è riportato un esempio di pass-through SSL:

```
frontend s3
       mode tcp
       bind *:443
       default_backend s3-servers
backend s3-servers
       balance leastconn
       option httpchk
       http-check expect status 200
       server dc1-s1 10.63.174.71:18082 check-ssl verify none inter 3000
       server dc1-s2 10.63.174.72:18082 check-ssl verify none inter 3000
       server dc1-s3 10.63.174.73:18082 check-ssl verify none inter 3000
```

Per esempi completi di configurazioni per StorageGRID, vedere "Esempi di configurazione HAProxy" su GitHub.

Convalidare la connessione SSL in StorageGRID

Informazioni su come convalidare la connessione SSL in StorageGRID.

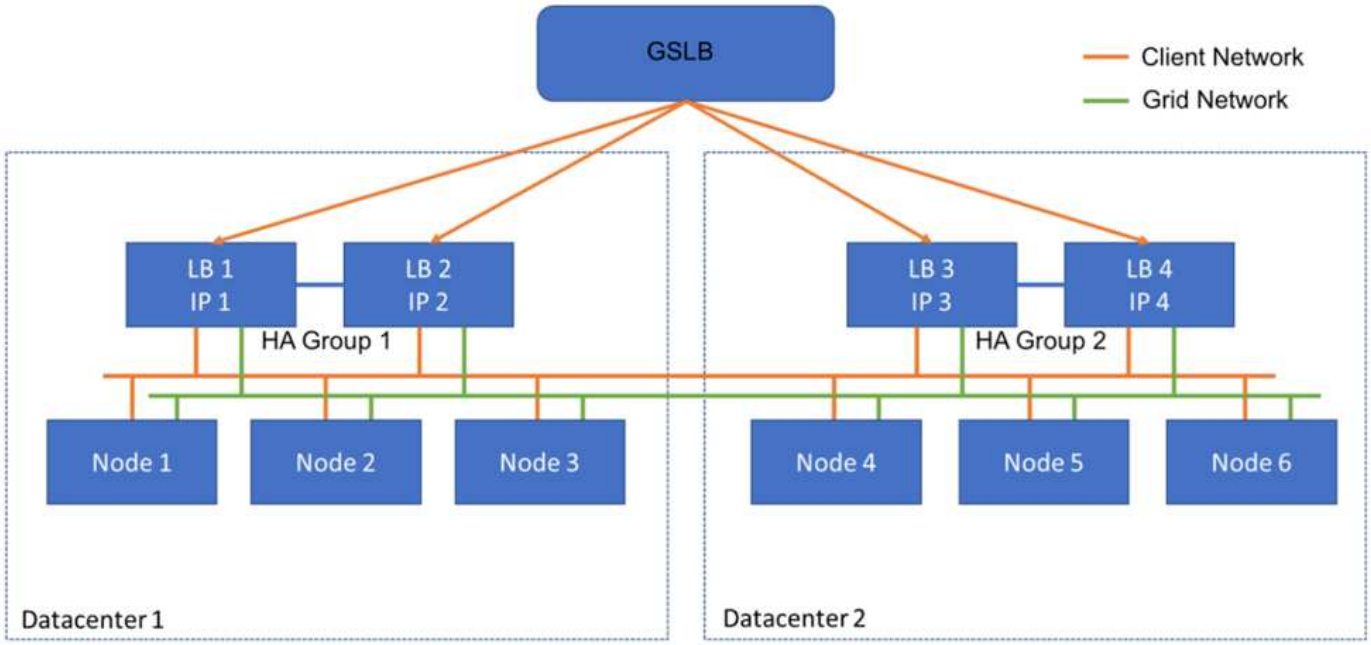
Una volta configurato il bilanciamento del carico, è necessario convalidare la connessione utilizzando strumenti come OpenSSL e l'interfaccia CLI di AWS. Altre applicazioni, come il browser S3, potrebbero ignorare errori di configurazione SSL.

Comprendere i requisiti globali di bilanciamento del carico per StorageGRID

Esplorate le considerazioni e i requisiti di progettazione per il bilanciamento del carico globale in StorageGRID.

Il bilanciamento del carico globale richiede l'integrazione con DNS per fornire routing intelligente su più siti StorageGRID. Questa funzione si trova al di fuori del dominio StorageGRID e deve essere fornita da una soluzione di terze parti come i prodotti di bilanciamento del carico discussi in precedenza e/o una soluzione di controllo del traffico DNS come Infoblox. Il bilanciamento del carico di livello superiore fornisce un routing

intelligente al sito di destinazione più vicino nello spazio dei nomi, nonché il rilevamento e il reindirizzamento dei black-out al sito successivo nello spazio dei nomi. Una tipica implementazione GSLB è costituita dal GSLB di livello superiore con pool di siti contenenti bilanciatori del carico locale-sito. I bilanciatori del carico del sito contengono pool di nodi di storage del sito locale. Ciò può includere una combinazione di bilanciatori del carico di terze parti per le funzioni GSLB e StorageGRID che fornisce il bilanciamento del carico locale del sito, o una combinazione di terze parti, o molte delle terze parti discusse in precedenza possono fornire bilanciamento del carico sia GSLB che locale del sito.



TR-4645: Funzionalità di sicurezza

Proteggi dati e metadati StorageGRID in un archivio di oggetti

Scopri le funzionalità di sicurezza integrate della soluzione di storage a oggetti StorageGRID.

Questa è una panoramica delle numerose funzionalità di sicurezza di NetApp® StorageGRID®, che riguardano l'accesso ai dati, gli oggetti e i metadati, l'accesso amministrativo e la sicurezza della piattaforma. È stato aggiornato per includere le funzionalità più recenti rilasciate con StorageGRID 12.0.

La sicurezza è parte integrante della soluzione di storage a oggetti NetApp StorageGRID. La sicurezza è particolarmente importante, in quanto molti tipi di dati rich content adatti allo storage a oggetti sono anche sensibili, soggetti a normative e conformità. Con la continua evoluzione delle funzionalità di StorageGRID, il software rende disponibili molte funzionalità di sicurezza preziose per proteggere il livello di sicurezza di un'organizzazione e aiutare l'organizzazione a soddisfare le Best practice del settore.

Questo documento fornisce una panoramica delle numerose funzionalità di sicurezza di StorageGRID 12.0, suddivise in cinque categorie:

- Funzioni di sicurezza per l'accesso ai dati
- Funzionalità di sicurezza di oggetti e metadati
- Funzioni di protezione di amministrazione
- Funzioni di sicurezza della piattaforma

- Integrazione del cloud

Questo documento è concepito come una scheda tecnica sulla sicurezza e non descrive in dettaglio come configurare il sistema per supportare le funzionalità di sicurezza elencate al suo interno che non sono configurate per impostazione predefinita. IL "Guida alla tempra StorageGRID" è disponibile sul sito ufficiale "Documentazione StorageGRID" pagina.

Oltre alle funzionalità descritte in questo rapporto, StorageGRID segue la "Criteri di notifica e risposta alle vulnerabilità di protezione dei prodotti NetApp". Le vulnerabilità segnalate vengono verificate e risolte in base al processo di risposta agli incidenti di sicurezza del prodotto.

NetApp StorageGRID offre funzionalità di sicurezza avanzate per casi di utilizzo dello storage a oggetti aziendale molto esigenti.

Dove trovare ulteriori informazioni

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

- NetApp StorageGRID: Valutazione della conformità SEC 17a-4(f), FINRA 4511(c) e CFTC 1,31(c)-(d) https://www.netapp.com/media/9041-ar-cohasset-netapp-storagegrid-sec-assessment.pdf
- Certificazione NIST FIPS 140-3 Kernel Crypto NetApp StorageGRID https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/5097
- Certificazione entropia NIST SP 800-90B NetApp StorageGRID https://csrc.nist.gov/projects/cryptographic-module-validation-program/entropy-validations/certificate/223
- Certificazione Common Criteria del Centro canadese per la sicurezza informatica NetApp StorageGRID https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/565-LSS%20CT%20v1.0.pdf
- Pagina della documentazione StorageGRIDhttps://docs.netapp.com/us-en/storagegrid/[]
- Documentazione dei prodotti NetApp https://www.netapp.com/support-and-training/documentation/

Termini e acronimi

In questa sezione vengono fornite le definizioni della terminologia utilizzata nel documento.

Termine o acronimo	Definizione
S3	Simple Storage Service.
Client	Applicazione in grado di interfacciarsi con StorageGRID tramite il protocollo S3 per l'accesso ai dati o il protocollo HTTP per la gestione.
Amministratore tenant	L'amministratore dell'account tenant StorageGRID
Utente tenant	Un utente all'interno di un account tenant StorageGRID
TLS	Transport Layer Security
ILM	Gestione del ciclo di vita delle informazioni
LAN	Local Area Network (rete locale)
Amministratore di grid	L'amministratore del sistema StorageGRID
Griglia	Il sistema StorageGRID

Termine o acronimo	Definizione
Bucket	Un contenitore per gli oggetti memorizzati in S3
LDAP	Lightweight Directory Access Protocol
SEC.	Securities and Exchange Commission; regola i membri di Exchange, i broker o i dealer
FINRA	Autorità di regolamentazione del settore finanziario; difende i requisiti di formato e media della norma SEC 17a-4(f)
CFTC	Commodity Futures Trading Commission; regola il commodity futures trading
NIST	Istituto Nazionale di Standard e tecnologia

Funzioni di sicurezza per l’accesso ai dati

Scopri le funzionalità di sicurezza dell’accesso ai dati di StorageGRID.

Funzione	Funzione	Impatto	Conformità normativa
TLS (Transport Layer Security) configurabile	TLS stabilisce un protocollo di handshake per la comunicazione tra un client e un nodo di gateway StorageGRID, un nodo storage o un endpoint del bilanciamento del carico. StorageGRID supporta le seguenti suite di crittografia per TLS: • TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • TLS_AES_256_GCM_SHA384 • DHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • AES128-GCM-SHA256 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-CHACHA20-POLY1305 • ECDHE-RSA-CHACHA20-POLY1305 Supporto di TLS v1,2 e 1,3. SSLv3, TLS v1.1 e versioni precedenti non sono supportati.	Consente a un client e a StorageGRID di identificarsi e autenticarsi reciprocamente e comunicare con riservatezza e integrità dei dati. Garantisce l'uso di una versione TLS recente. Le crittografie sono ora configurabili nelle impostazioni di configurazione/protezione	—

Funzione	Funzione	Impatto	Conformità normativa
Certificato server configurabile (endpoint bilanciamento del carico)	Gli amministratori di grid possono configurare gli endpoint di Load Balancer in modo da generare o utilizzare un certificato server.	Consente l'utilizzo di certificati digitali firmati dalla propria autorità di certificazione (CA) standard per autenticare le operazioni API degli oggetti tra la griglia e il client per ogni endpoint di bilanciamento del carico.	—
Certificato server configurabile (endpoint API)	Gli amministratori della griglia possono configurare centralmente tutti gli endpoint delle API StorageGRID in modo che utilizzino un certificato server firmato dalla CA attendibile dell'organizzazione.	Consente l'utilizzo di certificati digitali firmati dalla CA standard e attendibile per autenticare le operazioni API degli oggetti tra un client e la griglia.	—

Funzione	Funzione	Impatto	Conformità normativa
Multi-tenancy	StorageGRID supporta tenant multipli per grid e ogni tenant ha il proprio namespace. Un tenant offre un protocollo S3:1; per impostazione predefinita, l'accesso a bucket/container e oggetti è limitato agli utenti all'interno dell'account. I tenant possono avere un utente (ad esempio, un'implementazione aziendale, in cui ogni utente ha un proprio account) o più utenti (ad esempio, un'implementazione di un provider di servizi, in cui ogni account è un'azienda e un cliente del provider di servizi). Gli utenti possono essere locali o federati; gli utenti federati sono definiti da Active Directory o LDAP (Lightweight Directory Access Protocol). StorageGRID fornisce una dashboard per tenant, in cui gli utenti accedono utilizzando le credenziali dell'account locale o federato. Gli utenti possono accedere ai report visualizzati sull'utilizzo del tenant rispetto alla quota assegnata dall'amministratore del grid, incluse le informazioni sull'utilizzo nei dati e negli oggetti archiviati dai bucket. Gli utenti con autorizzazioni amministrative possono eseguire attività di amministrazione del sistema a livello di tenant, come la gestione di utenti, gruppi e chiavi di accesso.	Consente agli amministratori di StorageGRID di ospitare i dati da più tenant isolando al contempo l'accesso al tenant e di stabilire l'identità dell'utente federando gli utenti con un provider di identità esterno, come Active Directory o LDAP.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Mancata pubblicazione delle credenziali di accesso	Ogni operazione S3 viene identificata e registrata con un account tenant, un utente e una chiave di accesso univoci.	Consente agli amministratori Grid di stabilire quali azioni API vengono eseguite da ciascun utente.	—

Funzione	Funzione	Impatto	Conformità normativa
Accesso anonimo disattivato	Per impostazione predefinita, l'accesso anonimo è disattivato per gli account S3. Un richiedente deve disporre di una credenziale di accesso valida per un utente valido nell'account tenant per accedere a bucket, contenitori o oggetti all'interno dell'account. L'accesso anonimo a bucket o oggetti S3 può essere abilitato con un criterio IAM esplicito.	Consente agli amministratori Grid di disabilitare o controllare l'accesso anonimo a bucket/container e oggetti.	—
WORM di conformità	Progettato per soddisfare i requisiti della norma SEC 17a-4(f) e convalidato da Cohasset. I clienti possono garantire la conformità a livello della benna. La ritenzione può essere estesa ma mai ridotta. Le regole di Information Lifecycle management (ILM) applicano livelli minimi di protezione dei dati.	Consente ai tenant con requisiti di data retention normativi per consentire protezione WORM su oggetti memorizzati e metadati di oggetti.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
WORM	Gli amministratori di grid possono abilitare IL WORM a livello di griglia attivando l'opzione Disattiva modifica client, che impedisce ai client di sovrascrivere o eliminare oggetti o metadati di oggetti in tutti gli account tenant. Gli amministratori dei tenant S3 possono inoltre abilitare il WORM in base al tenant, bucket o prefisso dell'oggetto specificando il criterio IAM, che include l'autorizzazione personalizzata S3: PutOverwriteObject per la sovrascrittura di oggetti e metadati.	Permette agli amministratori di Grid e agli amministratori dei tenant di controllare la protezione WORM su oggetti archiviati e metadati di oggetti.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)

Funzione	Funzione	Impatto	Conformità normativa
Gestione della chiave di crittografia del server host KMS	Gli amministratori di grid possono configurare uno o più server KMS (External Key Management Server) in Grid Manager in modo da fornire chiavi di crittografia ai servizi StorageGRID e alle appliance di storage. Ogni server host KMS o cluster di server host KMS utilizza il Key Management Interoperability Protocol (KMIP) per fornire una chiave di crittografia ai nodi di appliance nel sito StorageGRID associato.	Crittografia dei dati a riposo attivata. Una volta crittografati i volumi dell'appliance, non è possibile accedere ai dati sull'appliance a meno che il nodo non sia in grado di comunicare con il server host KMS.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Failover automatico	StorageGRID offre ridondanza integrata e failover automatizzato. L'accesso ad account, bucket e oggetti tenant può continuare anche in caso di guasti multipli, da dischi o nodi a interi siti. StorageGRID è consapevole delle risorse e reindirizza automaticamente le richieste ai nodi disponibili e alle posizioni dei dati. I siti StorageGRID possono persino funzionare in modalità island; se un'interruzione della WAN disconnette un sito dal resto del sistema, le letture e le scritture possono continuare con le risorse locali e la replica riprende automaticamente quando la WAN viene ripristinata.	Consente agli amministratori Grid di gestire i tempi di attività, gli SLA e altri obblighi contrattuali e di implementare i piani di business continuity.	—
Funzionalità di protezione dell'accesso ai dati specifiche per S3	Firma AWS versione 2 e versione 4	La firma delle richieste API fornisce l'autenticazione per le operazioni API S3. Amazon supporta due versioni di Signature versione 2 e 4. Il processo di firma verifica l'identità del richiedente, protegge i dati in transito e protegge da potenziali attacchi di riproduzione.	Si allinea al suggerimento AWS per la versione Signature 4 e consente la compatibilità con le versioni precedenti delle applicazioni con la versione Signature 2.

Funzione	Funzione	Impatto	Conformità normativa
—	Blocco oggetti S3	La funzionalità blocco oggetti S3 in StorageGRID è una soluzione di protezione degli oggetti equivalente a blocco oggetti S3 in Amazon S3.	Consente ai tenant di creare bucket con blocco oggetti S3 abilitato per la conformità alle normative che richiedono la conservazione di determinati oggetti per un periodo di tempo fisso o indefinitamente.
Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)	Archiviazione protetta di credenziali S3	Le chiavi di accesso S3 sono memorizzate in un formato protetto da una funzione di hashing di password (SHA-2).	Consente l'archiviazione protetta delle chiavi di accesso mediante una combinazione di lunghezza della chiave (un numero generato casualmente da 10^{31}) e un algoritmo di hash delle password.
—	S3 tasti di accesso con limite di tempo	Quando si crea una chiave di accesso S3 per un utente, i clienti possono impostare una data e un'ora di scadenza sulla chiave di accesso.	Offre agli amministratori Grid la possibilità di fornire chiavi di accesso S3 temporanee.
—	Più chiavi di accesso per account utente	StorageGRID consente di creare più chiavi di accesso e contemporaneamente di attivarle per un account utente. Poiché ogni azione API viene registrata con un account utente tenant e una chiave di accesso, la non ripubblicazione viene mantenuta nonostante siano attive più chiavi.	Consente ai client di ruotare le chiavi di accesso senza interruzioni e consente a ciascun client di disporre della propria chiave, scoraggiando la condivisione delle chiavi tra i client.

Funzione	Funzione	Impatto	Conformità normativa
—	S3 criterio di accesso IAM	StorageGRID supporta policy IAM S3, consentendo agli amministratori Grid di specificare un controllo granulare degli accessi per tenant, bucket o prefisso oggetto. StorageGRID supporta inoltre le variabili e le condizioni dei criteri IAM, consentendo criteri di controllo degli accessi più dinamici.	Consente agli amministratori di Grid di specificare il controllo dell'accesso per gruppi di utenti per l'intero tenant; inoltre, permette agli utenti tenant di specificare il controllo dell'accesso per i propri bucket e oggetti.
—	API del servizio token di sicurezza S3 AssumeRole	StorageGRID supporta l'API S3 STS AssumeRole per fornire credenziali di sicurezza temporanee (ID chiave di accesso, chiave di accesso segreta, token di sessione) con autorizzazioni ridotte e durata limitata. Come parte dell'API AssumeRole sono supportati criteri di sessione in linea per limitare ulteriormente le autorizzazioni durante la sessione.	Consente agli amministratori dei tenant di fornire un accesso temporaneo sicuro ai dati degli oggetti.
—	Servizio di notifica semplice	StorageGRID supporta l'invio di notifiche sull'accesso agli oggetti. Sono supportati i seguenti tipi di eventi: • s3:OggettoCreato: • s3:OggettoCreato:Metti • s3:OggettoCreato:Post • s3:OggettoCreato:Copia • s3:ObjectCreated:CompleteMultipartUpload • s3:ObjectRemoved: • s3:ObjectRemoved:Elimina • s3:ObjectRemoved:DeleteMarkerCreated • s3:ObjectRestore:Post	Consente agli amministratori dei tenant di monitorare l'accesso agli oggetti

Funzione	Funzione	Impatto	Conformità normativa
—	Crittografia lato server con chiavi gestite da StorageGRID (SSE)	StorageGRID supporta SSE, consentendo una protezione multitenant dei dati a riposo con chiavi di crittografia gestite da StorageGRID.	Consente ai tenant di crittografare gli oggetti. La chiave di crittografia è necessaria per scrivere e recuperare questi oggetti.
Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)	Crittografia lato server con chiavi di crittografia fornite dal cliente (SSE-C)	StorageGRID supporta SSE-C, abilitando la protezione multitenant dei dati a riposo con chiavi di crittografia gestite dal client. Sebbene StorageGRID gestisca tutte le operazioni di crittografia e decrittografia degli oggetti, con SSE-C, il client deve gestire autonomamente le chiavi di crittografia.	Consente ai client di crittografare gli oggetti con le chiavi controllate dall'utente. La chiave di crittografia è necessaria per scrivere e recuperare questi oggetti.

Sicurezza di oggetti e metadati

Esplora le funzionalità di sicurezza degli oggetti e dei metadati in StorageGRID.

Funzione	Funzione	Impatto	Conformità normativa
Crittografia degli oggetti lato server AES (Advanced Encryption Standard)	StorageGRID fornisce la crittografia degli oggetti sul lato server basata su AES 128 e AES 256. Gli amministratori della griglia possono abilitare la crittografia come impostazione predefinita globale. StorageGRID supporta inoltre l'intestazione di crittografia S3 x-amz-lato server per consentire l'attivazione o la disattivazione della crittografia in base all'oggetto. Se abilitato, gli oggetti vengono crittografati quando vengono archiviati o in transito tra i nodi della griglia.	Aiuta a proteggere lo storage e la trasmissione degli oggetti, indipendentemente dall'hardware per lo storage sottostante.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)

Funzione	Funzione	Impatto	Conformità normativa
Gestione delle chiavi integrata	Quando la crittografia è attivata, ogni oggetto viene crittografato con una chiave simmetrica univoca generata in modo casuale, memorizzata all'interno di StorageGRID senza accesso esterno.	Consente la crittografia degli oggetti senza richiedere una gestione esterna delle chiavi.	
Dischi di crittografia conformi a Federal Information Processing Standard (FIPS) 140-2-2	Le appliance SG5812, SG5860, SG6160 e SGF6024 StorageGRID offrono l'opzione di dischi di crittografia conformi FIPS 140-2-2. Le chiavi di crittografia dei dischi possono essere facoltativamente gestite da un server KMIP esterno.	Abilita lo storage sicuro di dati, metadati e oggetti di sistema. Fornisce inoltre una crittografia degli oggetti basata su software StorageGRID, che protegge storage e trasmissione di oggetti.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Crittografia conforme allo standard federale di elaborazione delle informazioni (FIPS) 140-3 per i nodi	Gli appliance StorageGRID SG5812, SG5860, SG6160, SGF6112, SG1100 e SG110 offrono l'opzione di crittografia dei nodi conforme allo standard FIPS 140-3. Le chiavi di crittografia per i nodi sono gestite da un server KMIP esterno.	Abilita lo storage sicuro di dati, metadati e oggetti di sistema. Fornisce inoltre una crittografia degli oggetti basata su software StorageGRID, che protegge storage e trasmissione di oggetti.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Scansione di integrità in background e autoriparazione	StorageGRID utilizza un meccanismo di interblocco costituito da hash, checksum e controlli di ridondanza ciclici (CRC) a livello di oggetto e sottooggetto per proteggere da incoerenza, manomissioni o modifiche dei dati, sia quando gli oggetti sono in storage che in transito. StorageGRID rileva automaticamente gli oggetti corrotti e manomessi e li sostituisce, mettendo in quarantena i dati modificati e avvisando l'amministratore.	Permette agli amministratori di grid di soddisfare SLA, normative e altri obblighi in termini di conservazione dei dati. Aiuta i clienti a rilevare ransomware o virus che tentano di crittografare, manomettere o modificare i dati.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)

Funzione	Funzione	Impatto	Conformità normativa
Conservazione e posizionamento degli oggetti basati su policy	StorageGRID consente agli amministratori di grid di configurare regole ILM che specificano conservazione, posizionamento, protezione, transizione e scadenza degli oggetti. Gli amministratori del grid possono configurare StorageGRID per filtrare gli oggetti in base ai propri metadati e applicare regole a vari livelli di granularità, tra cui Grid-wide, tenant, bucket, key prefix, coppie di valori chiave e metadati definiti dall'utente. StorageGRID contribuisce a garantire che gli oggetti vengano memorizzati in base alle regole ILM durante il loro ciclo di vita, a meno che non vengano esplicitamente eliminati dal client.	Aiuta ad applicare il posizionamento, la protezione e la conservazione dei dati. Aiuta i clienti a raggiungere gli SLA relativi a durata, disponibilità e performance.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Scansione dei metadati in background	StorageGRID esegue periodicamente la scansione dei metadati degli oggetti in background per applicare modifiche al posizionamento o alla protezione dei dati degli oggetti come specificato da ILM.	Aiuta a rilevare gli oggetti danneggiati.	
Uniformità regolabile	I tenant possono selezionare livelli di coerenza a livello del bucket per garantire che siano disponibili risorse come la connettività multisito.	Offre l'opzione per eseguire il commit delle scritture sulla griglia solo quando è disponibile un numero richiesto di siti o risorse.	

Funzioni di protezione di amministrazione

Scoprite le funzioni di protezione dell'amministrazione in StorageGRID.

Funzione	Funzione	Impatto	Conformità normativa
Certificato server (Grid Management Interface)	Gli amministratori di rete possono configurare Grid Management Interface in modo che utilizzi un certificato server firmato dalla CA attendibile dell'organizzazione.	Consente l'utilizzo di certificati digitali firmati dalla CA standard e attendibile per autenticare l'accesso all'interfaccia utente di gestione e all'API tra un client di gestione e la griglia.	—
Autenticazione utente amministrativo	Gli utenti amministrativi vengono autenticati utilizzando il nome utente e la password. Gli utenti e i gruppi amministrativi possono essere locali o federati, importati da Active Directory o LDAP del cliente. Le password degli account locali sono memorizzate in un formato protetto da bcrypt; le password della riga di comando sono memorizzate in un formato protetto da SHA-2.	Autentica l'accesso amministrativo alla UI di gestione e alle API.	—
Supporto SAML	StorageGRID supporta il single sign-on (SSO) utilizzando lo standard SAML 2,0 (Security Assertion Markup Language 2,0). Quando SSO è attivato, tutti gli utenti devono essere autenticati da un provider di identità esterno prima di poter accedere a Grid Manager, Tenant Manager, Grid Management API o Tenant Management API. Gli utenti locali non possono accedere a StorageGRID.	Offre livelli aggiuntivi di sicurezza per gli amministratori di tenant e grid come SSO e Multifactor Authentication (MFA).	NIST SP800-63
Controllo granulare delle autorizzazioni	Gli amministratori Grid possono assegnare autorizzazioni ai ruoli e assegnare ruoli a gruppi di utenti amministrativi, in base alle attività a cui i client amministrativi possono eseguire utilizzando sia l'interfaccia utente di gestione che le API.	Consente agli amministratori Grid di gestire il controllo degli accessi per gli utenti e i gruppi amministrativi.	—

Funzione	Funzione	Impatto	Conformità normativa
Registrazione di controllo distribuita	StorageGRID fornisce un'infrastruttura integrata di registrazione degli audit distribuita, scalabile fino a centinaia di nodi in un massimo di 16 siti. I nodi software StorageGRID generano messaggi di audit, che vengono trasmessi attraverso un sistema di inoltro di audit ridondante e infine acquisiti in uno o più repository di audit log. I messaggi di audit acquisiscono eventi a livello di granularità degli oggetti, come operazioni API S3 avviate dal client, eventi del ciclo di vita degli oggetti da ILM, controlli dello stato di salute degli oggetti in background e modifiche della configurazione effettuate dall'interfaccia utente di gestione o dalle API. I registri di controllo possono essere esportati tramite syslog, consentendo l'analisi dei messaggi di controllo tramite strumenti quali Splunk ed ELK. Esistono quattro tipi di messaggi di controllo: • Messaggi di audit del sistema • Messaggi di audit dello storage a oggetti • Messaggi di controllo del protocollo HTTP • Gestione dei messaggi di controllo I registri di controllo possono essere archiviati in un bucket S3 per la conservazione a lungo termine e l'accesso alle applicazioni.	Fornisce agli amministratori Grid un servizio di controllo collaudato e scalabile e consente loro di estrarre i dati di controllo per vari obiettivi. Tali obiettivi includono la risoluzione dei problemi, il controllo delle prestazioni dello SLA, le operazioni API di accesso ai dati dei client e le modifiche alla configurazione di gestione.	—

Funzione	Funzione	Impatto	Conformità normativa
Audit del sistema	I messaggi di controllo del sistema acquisiscono gli eventi correlati al sistema, come gli stati dei nodi della griglia, il rilevamento degli oggetti corrotti, gli oggetti sottoposti a commit in tutte le posizioni specificate per la regola ILM e l'avanzamento delle attività di manutenzione a livello di sistema (attività griglia).	Aiuta i clienti a risolvere i problemi del sistema e fornisce la prova che gli oggetti vengono memorizzati in base al loro SLA. Gli SLA sono implementati dalle regole ILM di StorageGRID e protetti dall'integrità.	—
Verifica dello storage a oggetti	I messaggi di audit dello storage a oggetti acquisiscono la transazione di API a oggetti e gli eventi relativi al ciclo di vita. Questi eventi includono storage e recupero di oggetti, trasferimenti da grid-node a grid-node e verifiche.	Aiuta i clienti a controllare lo stato di avanzamento dei dati nel sistema e se gli SLA, specificati come StorageGRID ILM, vengono erogati.	—
Controllo del protocollo HTTP	I messaggi di controllo del protocollo HTTP acquisiscono le interazioni del protocollo HTTP correlate alle applicazioni client e ai nodi StorageGRID. Inoltre, i clienti possono acquisire intestazioni specifiche delle richieste HTTP (ad esempio, X-Forwarding-for e metadati utente [x-amz-meta-*]) nella verifica.	Aiuta i clienti a controllare le operazioni API di accesso ai dati tra client e StorageGRID e a tracciare un'azione per un account utente e una chiave di accesso individuali. I clienti possono anche registrare i metadati degli utenti nelle verifiche e utilizzare strumenti di log mining come Splunk o ELK, per cercare i metadati degli oggetti.	—
Audit di gestione	I messaggi di controllo di gestione registrano le richieste degli utenti amministrativi all'interfaccia utente di gestione (Grid Management Interface) o alle API. Ogni richiesta che non è UNA richiesta GET o HEAD all'API registra una risposta con il nome utente, l'IP e il tipo di richiesta all'API.	Aiuta gli amministratori Grid a stabilire un record delle modifiche alla configurazione del sistema apportate dall'utente da quale IP di origine e quale IP di destinazione in quale momento.	—

Funzione	Funzione	Impatto	Conformità normativa
Supporto TLS 1,3 per l'interfaccia utente di gestione e l'accesso API	TLS stabilisce un protocollo handshake per la comunicazione tra un client admin e un nodo admin StorageGRID.	Consente a un client amministrativo e a StorageGRID di identificarsi e autenticarsi reciprocamente e comunicare con riservatezza e integrità dei dati.	—
SNMPv3 per il monitoraggio StorageGRID	SNMPv3 garantisce la sicurezza offrendo autenticazione avanzata e crittografia dei dati per la privacy. Con v3, le unità dei dati del protocollo vengono crittografate utilizzando CBC-DES per il protocollo di crittografia. L'autenticazione dell'utente di chi ha inviato l'unità dati del protocollo è fornita dal protocollo di autenticazione HMAC-SHA o HMAC-MD5. SNMPv2 e v1 sono ancora supportati.	Aiuta gli amministratori di rete a monitorare il sistema StorageGRID abilitando un agente SNMP sul nodo Admin.	—
Certificati client per l'esportazione delle metriche Prometheus	Gli amministratori di rete possono caricare o generare certificati client che possono essere utilizzati per fornire un accesso sicuro e autenticato al database StorageGRID Prometheus.	Gli amministratori di rete possono utilizzare i certificati client per monitorare StorageGRID esternamente utilizzando applicazioni come Grafana.	—

Funzioni di sicurezza della piattaforma

Informazioni sulle funzionalità di sicurezza della piattaforma in StorageGRID.

Funzione	Funzione	Impatto	Conformità normativa
Infrastruttura a chiave pubblica (PKI) interna, certificati dei nodi e TLS	StorageGRID utilizza un'infrastruttura PKI interna e certificati di nodo per autenticare e crittografare la comunicazione internodale. La comunicazione internodale è protetta da TLS.	Contribuisce a proteggere il traffico del sistema su LAN o WAN, soprattutto in un'implementazione multisito.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)

Funzione	Funzione	Impatto	Conformità normativa
Firewall nodo	StorageGRID configura automaticamente le tabelle IP e le regole di firewall per controllare il traffico di rete in entrata e in uscita, oltre a chiudere le porte non utilizzate.	Consente di proteggere il sistema StorageGRID, i dati e i metadati dal traffico di rete non richiesto.	—
Protezione avanzata dei sistemi operativi	Il sistema operativo di base delle appliance fisiche e dei nodi virtuali StorageGRID è rafforzato; vengono rimossi i pacchetti software non correlati.	Contribuisce a ridurre al minimo le potenziali superfici di attacco.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Aggiornamenti periodici della piattaforma e del software	StorageGRID fornisce versioni software regolari che includono il sistema operativo, i file binari delle applicazioni e gli aggiornamenti software.	Aiuta a mantenere il sistema StorageGRID aggiornato con i software e i file binari delle applicazioni correnti.	—
Accesso root disabilitato su Secure Shell (SSH)	Il login root su SSH è disabilitato su tutti i nodi StorageGRID. L'accesso SSH utilizza l'autenticazione del certificato.	Aiuta i clienti a proteggersi da potenziali violazioni remote delle password del login root.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Sincronizzazione automatica dell'ora	StorageGRID sincronizza automaticamente gli orologi di sistema di ciascun nodo con più server NTP (Time Network Protocol) esterni. Sono necessari almeno quattro server NTP di strato 3 o successivo.	Garantisce lo stesso riferimento temporale in tutti i nodi.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Separare le reti per il traffico grid interno, amministrativo e client	I nodi software e le appliance hardware StorageGRID supportano più interfacce di rete virtuali e fisiche, in modo che i clienti possano separare il traffico di client, amministrazione e rete interna su reti diverse.	Consenti agli amministratori Grid di separare il traffico di rete interno ed esterno e di distribuire il traffico sulle reti con SLA diversi.	—
Interfacce VLAN (Virtual LAN) multiple	StorageGRID supporta la configurazione delle interfacce VLAN sul client StorageGRID e sulle reti grid.	Consenti agli amministratori Grid di partizionare e isolare il traffico delle applicazioni per garantire sicurezza, flessibilità e prestazioni.	

Funzione	Funzione	Impatto	Conformità normativa
Rete client non attendibile	L'interfaccia di rete client non attendibile accetta connessioni in entrata solo su porte che sono state esplicitamente configurate come endpoint di bilanciamento del carico.	Garantisce la protezione delle interfacce esposte a reti non attendibili.	—
Firewall configurabile	Gestire le porte aperte e chiuse per le reti Admin, Grid e client.	Consentire agli amministratori di rete di controllare l'accesso alle porte e di gestire l'accesso alle porte dei dispositivi approvati.	
Comportamento SSH avanzato	disabilitare SSH per impostazione predefinita prima dell'installazione. Nello stato predefinito, l'accesso SSH è abilitato solo sull'indirizzo delle porte di gestione link-local. Le password utente admin e root sono impostate sul numero di serie del controller di elaborazione dell'appliance. L'accesso è consentito solo sulla console seriale e sulla console grafica (BMC KVM). SSH è disabilitato su qualsiasi porta di rete.	Migliora la protezione dell'accesso alla rete.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Crittografia dei nodi	Come parte della nuova funzione di crittografia del server host KMS, viene aggiunta una nuova impostazione di crittografia dei nodi al programma di installazione dell'appliance StorageGRID.	Questa impostazione deve essere attivata durante la fase di configurazione hardware dell'installazione dell'appliance.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)

Integrazione del cloud

Scopri come StorageGRID si integra con i servizi cloud.

Funzione	Funzione	Impatto
Scansione antivirus basata su notifiche	I servizi della piattaforma StorageGRID supportano le notifiche degli eventi. Le notifiche degli eventi possono essere utilizzate con servizi di cloud computing esterni per attivare i flussi di lavoro di scansione antivirus sui dati.	Consente agli amministratori dei tenant di attivare la scansione dei dati tramite virus utilizzando servizi di cloud computing esterni.

TR-4921: Difesa dal ransomware

Proteggere gli oggetti StorageGRID S3 dal ransomware

Scopri di più sugli attacchi ransomware e su come proteggere i dati grazie alle Best practice di sicurezza di StorageGRID.

Gli attacchi ransomware sono in aumento. Questo documento fornisce alcuni consigli su come proteggere i dati degli oggetti su StorageGRID.

Il ransomware di oggi è il pericolo sempre presente nel data center. Il ransomware è progettato per crittografare i dati e renderli inutilizzabili dagli utenti e dalle applicazioni che li fanno affidamento. La protezione inizia con le solite difese di reti rafforzate e solide pratiche di sicurezza per gli utenti, e dobbiamo seguire le procedure di sicurezza per l'accesso ai dati.

Il ransomware è una delle maggiori minacce alla sicurezza odierne. Il team NetApp StorageGRID collabora con i nostri clienti per stare al passo con queste minacce. Con l'uso del blocco degli oggetti e del controllo delle versioni, è possibile proteggere da modifiche indesiderate e ripristinare da attacchi dannosi. La sicurezza dei dati è un'impresa multi-layer che considera lo storage a oggetti solo una parte del data center.

Best practice di StorageGRID

Per StorageGRID, le Best practice sulla sicurezza devono includere l'utilizzo di HTTPS con certificati firmati sia per la gestione che per l'accesso agli oggetti. Crea account utente dedicati per applicazioni e singoli utenti e non utilizza gli account root tenant per l'accesso alle applicazioni o ai dati utente. In altre parole, seguire il principio del privilegio minimo. Utilizzare i gruppi di protezione con criteri IAM (Identity and Access Management) definiti per gestire i diritti degli utenti e accedere agli account specifici per le applicazioni e gli utenti. Con queste misure in atto, devi comunque assicurarti che i tuoi dati siano protetti. Nel caso di Simple Storage Service (S3), quando gli oggetti vengono modificati per crittografarli, viene eseguita la sovrascrittura dell'oggetto originale.

Metodi di difesa

Il meccanismo di protezione dal ransomware primario nell'API S3 consiste nell'implementare il blocco degli oggetti. Non tutte le applicazioni sono compatibili con il blocco degli oggetti, pertanto sono disponibili altre due opzioni per proteggere gli oggetti descritti in questo report: La replica in un altro bucket con la versione abilitata e la versione con i criteri IAM.

Dove trovare ulteriori informazioni

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

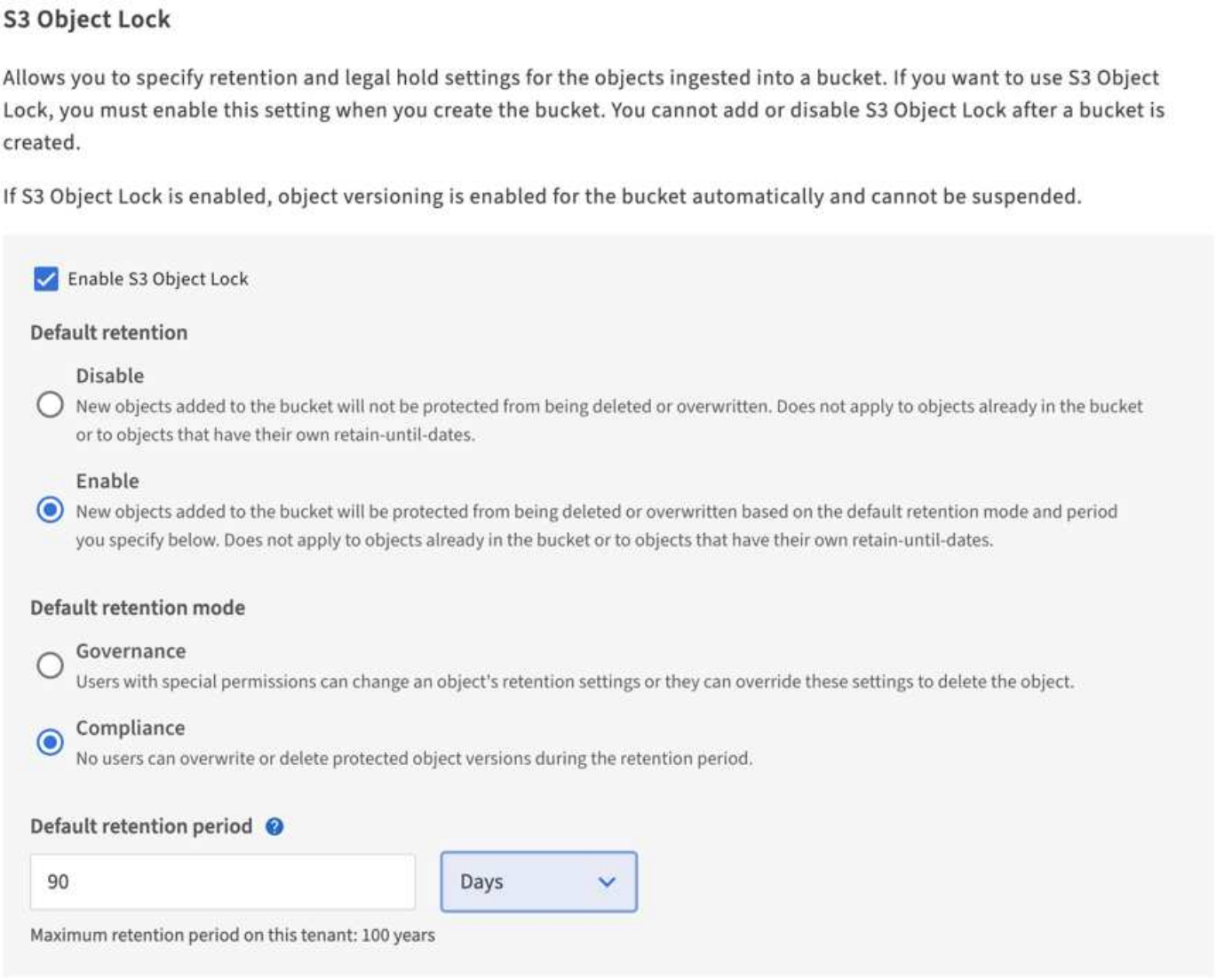
- Centro di documentazione NetApp StorageGRIDhttps://docs.netapp.com/us-en/storagegrid/[]
- Abilitazione NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Documentazione dei prodotti NetApp https://www.netapp.com/support-and-training/documentation/

Difesa dal ransomware tramite il blocco degli oggetti

Scopri come il blocco degli oggetti in StorageGRID fornisce un modello WORM per impedire la cancellazione o la sovrascrittura dei dati e come soddisfa i requisiti normativi.

Il blocco degli oggetti fornisce un modello WORM per impedire che gli oggetti vengano eliminati o sovrascritti. L'implementazione di StorageGRID del blocco degli oggetti è "Valutazione Cohasset" per aiutare a soddisfare i requisiti normativi, supportando la conservazione a fini giudiziari, la modalità di conformità e la modalità di governance per la conservazione degli oggetti e le policy di conservazione predefinite dei bucket. È necessario abilitare il blocco degli oggetti come parte della creazione e del controllo delle versioni del bucket. Una versione specifica di un oggetto è bloccata e, se non viene definito alcun ID di versione, la conservazione viene posizionata sulla versione corrente dell'oggetto. Se la versione corrente ha la conservazione configurata e si tenta di eliminare, modificare o sovrascrivere l'oggetto, viene creata una nuova versione con un marcatore di eliminazione o la nuova revisione dell'oggetto come versione corrente, e la versione bloccata viene mantenuta come una versione non corrente. Per le applicazioni non ancora compatibili, è comunque possibile utilizzare la configurazione di blocco degli oggetti e di conservazione predefinita inserita nel bucket. Una volta definita la configurazione, viene applicata una conservazione degli oggetti a ogni nuovo oggetto inserito nel bucket. Questa operazione funziona finché l'applicazione è configurata per non eliminare o sovrascrivere gli oggetti prima che sia trascorso il tempo di conservazione.

Quando si crea un bucket nell'interfaccia utente di gestione dei tenant, è possibile abilitare il blocco degli oggetti e configurare una modalità di conservazione predefinita e un periodo di conservazione. Se configurato, questo imposterà un blocco minimo di conservazione degli oggetti su ogni oggetto che viene inserito in quel bucket.



Di seguito sono riportati alcuni esempi di utilizzo dell'API di blocco degli oggetti:

Blocco oggetto conservazione legale è un semplice stato on/off applicato a un oggetto.

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal
-hold Status=ON --endpoint-url https://s3.company.com
```

L'impostazione dello stato di conservazione a fini giudiziari non restituisce alcun valore se l'operazione è riuscita, pertanto può essere verificata con un'operazione GET.

```
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "LegalHold": {
        "Status": "ON"
    }
}
```

Per disattivare la sospensione legale, applicare lo stato OFF.

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal
-hold Status=OFF --endpoint-url https://s3.company.com
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "LegalHold": {
        "Status": "OFF"
    }
}
```

L'impostazione della conservazione dell'oggetto viene eseguita con un Retain until timestamp.

```
aws s3api put-object-retention --bucket mybucket --key myfile.txt
--retention '{"Mode":"COMPLIANCE", "RetainUntilDate": "2022-06-
10T16:00:00"}'  --endpoint-url https://s3.company.com
```

Anche in questo caso, non viene restituito alcun valore in caso di esito positivo, pertanto è possibile verificare lo stato di conservazione in modo simile con una chiamata Get.

```
aws s3api get-object-retention --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-06-10T16:00:00+00:00"
    }
```

L'inserimento di una conservazione predefinita in un bucket abilitato per il blocco degli oggetti utilizza un periodo di conservazione in giorni e anni.

```
aws s3api put-object-lock-configuration --bucket mybucket --object-lock
-configuration '{ "ObjectLockEnabled": "Enabled", "Rule": {
"DefaultRetention": { "Mode": "COMPLIANCE", "Days": 1 }}}' --endpoint-url
https://s3.company.com
```

Come per la maggior parte di queste operazioni, non viene restituita alcuna risposta in caso di esito positivo, quindi è possibile eseguire un'operazione di RECUPERO per la verifica della configurazione.

```
aws s3api get-object-lock-configuration --bucket mybucket --endpoint-url
https://s3.company.com
{
    "ObjectLockConfiguration": {
        "ObjectLockEnabled": "Enabled",
        "Rule": {
            "DefaultRetention": {
                "Mode": "COMPLIANCE",
                "Days": 1
            }
        }
    }
}
```

Successivamente, è possibile inserire un oggetto nel bucket con la configurazione di conservazione applicata.

```
aws s3 cp myfile.txt s3://mybucket --endpoint-url https://s3.company.com
```

L'operazione PUT restituisce una risposta.

```
upload: ./myfile.txt to s3://mybucket/myfile.txt
```

Nell'oggetto Retention, la durata di conservazione impostata nel bucket nell'esempio precedente viene convertita in un timestamp di conservazione sull'oggetto.

```
aws s3api get-object-retention --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-03-02T15:22:47.202000+00:00"
    }
}
```

Difesa da ransomware tramite bucket replicati con versione

Scopri come replicare gli oggetti in un bucket secondario utilizzando StorageGRID CloudMirror.

Non tutte le applicazioni e i carichi di lavoro saranno compatibili con il blocco degli oggetti. Un'altra opzione è replicare gli oggetti in un bucket secondario nella stessa griglia (preferibilmente un tenant diverso con accesso limitato) o in qualsiasi altro endpoint S3 con il servizio della piattaforma StorageGRID, CloudMirror.

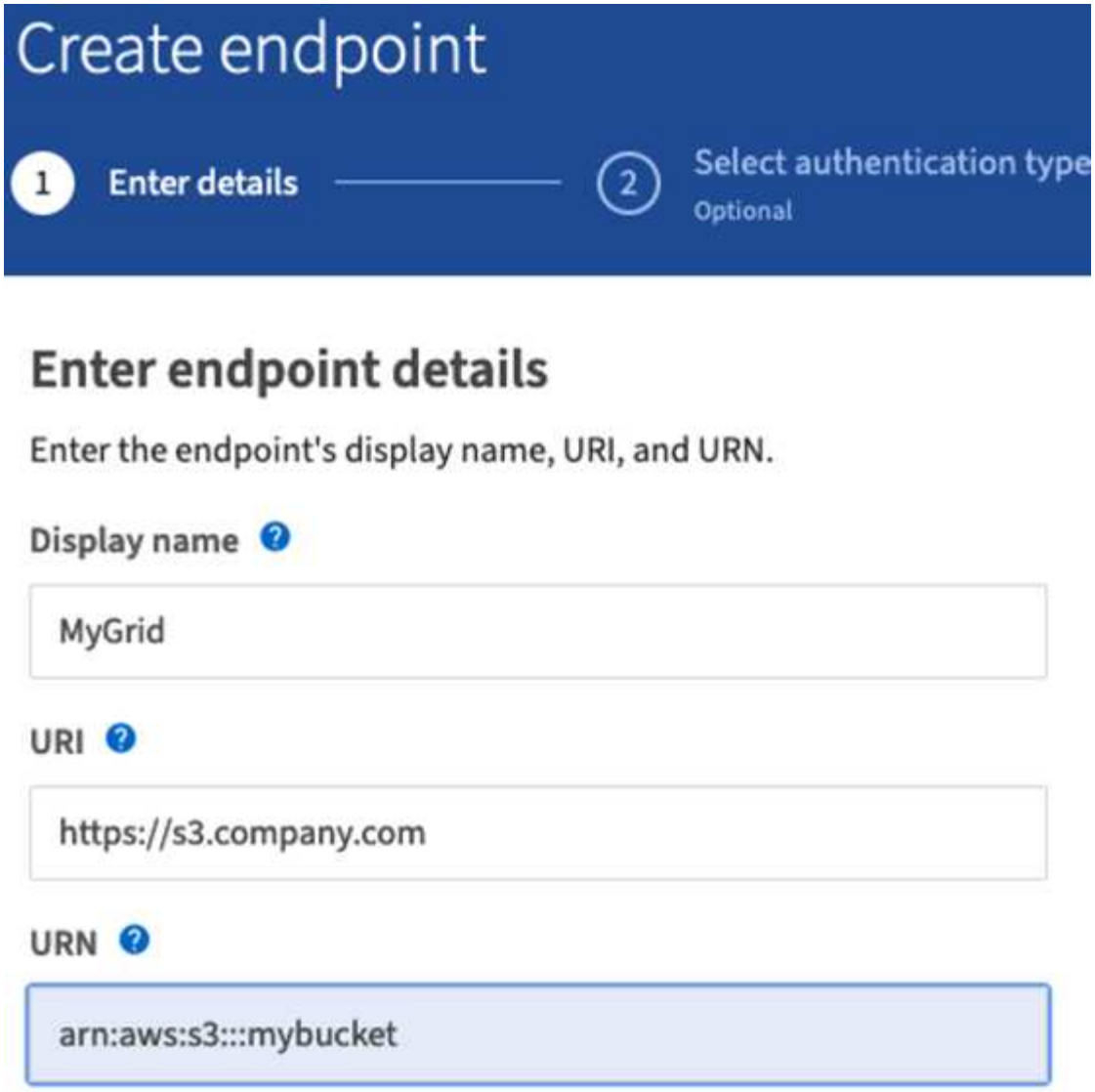
StorageGRID CloudMirror è un componente di StorageGRID che può essere configurato per replicare gli oggetti di un bucket in una destinazione definita quando vengono acquisiti nel bucket di origine e non replicano le eliminazioni. Poiché CloudMirror è un componente integrato di StorageGRID, non può essere disattivato o manipolato da un attacco basato su API S3. È possibile configurare questo bucket replicato con la versione abilitata. In questo scenario, è necessario eseguire una pulizia automatica delle vecchie versioni del bucket replicato, che possono essere eliminate in modo sicuro. A tale scopo, è possibile utilizzare il motore dei criteri ILM di StorageGRID. Creare regole per gestire il posizionamento degli oggetti in base al tempo non corrente per diversi giorni sufficienti ad identificarli e recuperarli da un attacco.

Un aspetto negativo di questo approccio è il fatto che consuma più storage disponendo di una seconda copia completa del bucket e di più versioni degli oggetti conservati per un po' di tempo. Inoltre, gli oggetti intenzionalmente eliminati dal bucket primario devono essere rimossi manualmente dal bucket replicato. Esistono altre opzioni di replica esterne al prodotto, come NetApp CloudSync, che possono replicare le eliminazioni per una soluzione simile. Un altro aspetto negativo per il bucket secondario che è abilitato per il controllo delle versioni e non per il blocco degli oggetti è la presenza di una serie di account privilegiati che potrebbero essere utilizzati per causare danni alla posizione secondaria. Il vantaggio è che dovrebbe essere un account univoco per quel bucket di endpoint o tenant e la compromissione probabilmente non include l'accesso agli account nella sede principale o viceversa.

Una volta creati i bucket di origine e destinazione e configurata la destinazione con la versione, è possibile configurare e abilitare la replica, come segue:

Fasi

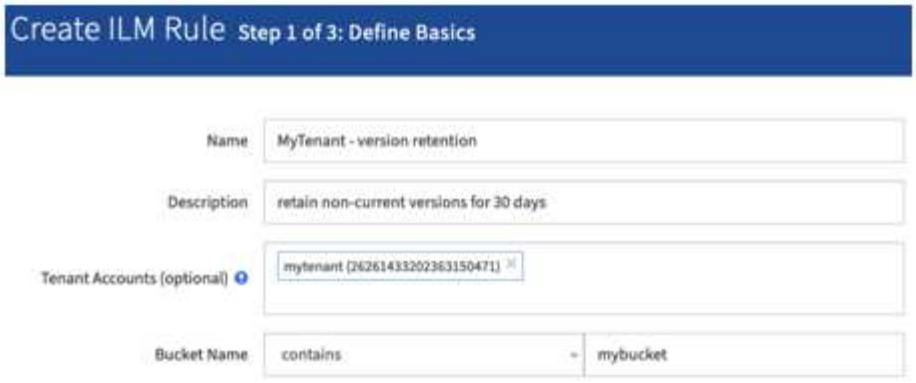
1. Per configurare CloudMirror, creare un endpoint dei servizi di piattaforma per la destinazione S3.

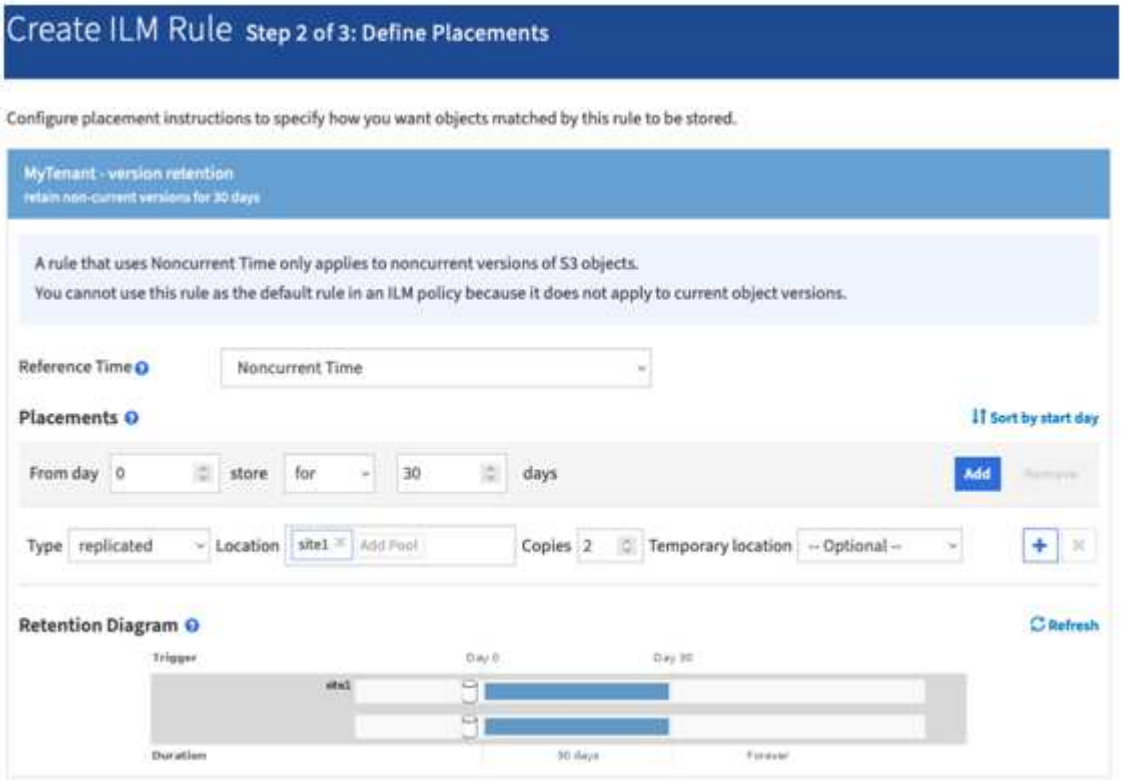


2. Nel bucket di origine, configurare la replica per utilizzare l'endpoint configurato.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
            <Bucket>arn:aws:s3:::mybucket</Bucket>
            <StorageClass>STANDARD</StorageClass>
        </Destination>
    </Rule>
</ReplicationConfiguration>
```

3. Creare regole ILM per gestire il posizionamento dello storage e la gestione della durata dello storage della versione. In questo esempio, vengono configurate le versioni non correnti degli oggetti da memorizzare.





Ci sono due copie nel sito 1 per 30 giorni. È inoltre possibile configurare le regole per la versione corrente degli oggetti in base all'utilizzo del tempo di acquisizione come tempo di riferimento nella regola ILM in modo che corrispondano alla durata di archiviazione del bucket di origine. Il posizionamento dello storage per le versioni a oggetti può essere sottoposto a erasure coding o replicato.

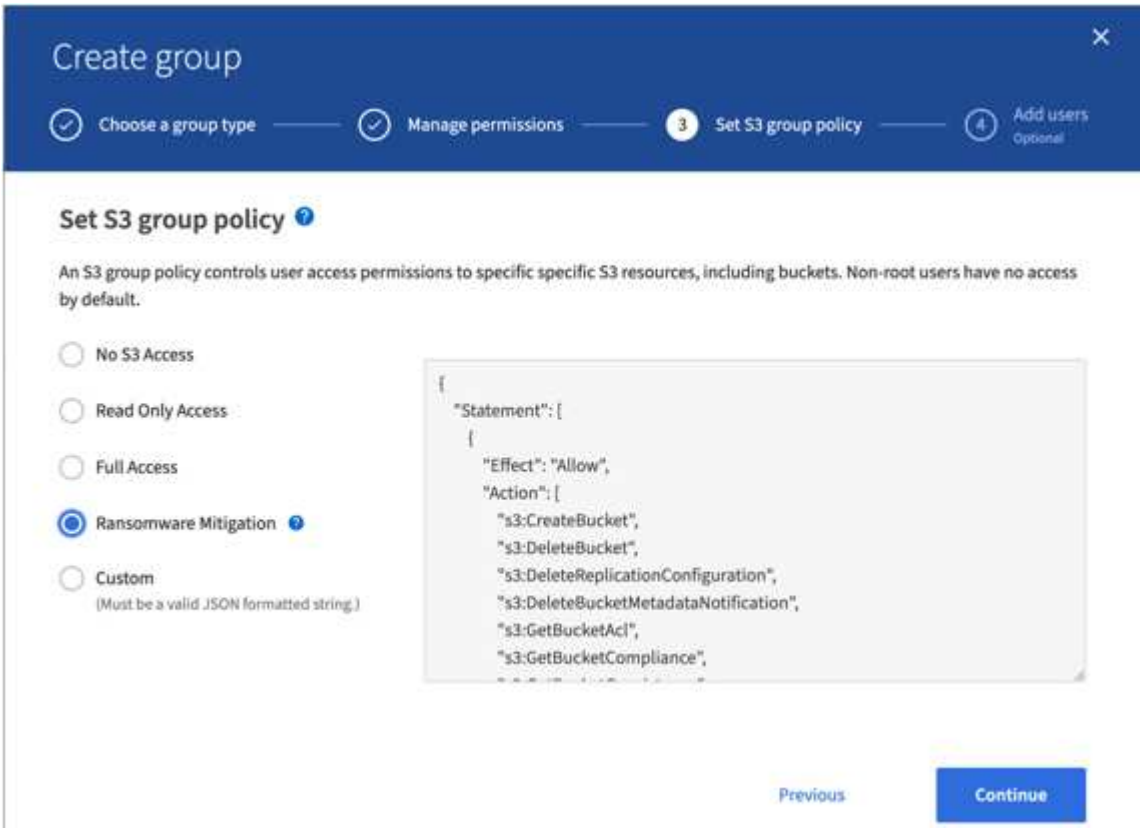
Difesa dal ransomware tramite versione con policy IAM di protezione

Scopri come proteggere i tuoi dati abilitando il controllo delle versioni nel bucket e implementando criteri IAM nei gruppi di sicurezza degli utenti in StorageGRID.

Un metodo per proteggere i dati senza utilizzare il blocco degli oggetti o la replica consiste nell'abilitare la versione nel bucket e implementare le policy IAM sui gruppi di sicurezza degli utenti per limitare la capacità degli utenti di gestire versioni degli oggetti. In caso di attacco, vengono create nuove versioni errate dei dati come la versione corrente e la versione non corrente più recente è quella sicura. Gli account compromessi per ottenere l'accesso ai dati non hanno accesso per eliminare o modificare in altro modo la versione non corrente

proteggendoli per operazioni di ripristino successive. Proprio come lo scenario precedente, le regole ILM gestiscono la conservazione delle versioni non correnti con una durata a scelta. L'aspetto negativo è che esiste ancora la possibilità di disporre di account privilegiati per un attacco di un attore non valido, ma tutti gli account del servizio applicazioni e gli utenti devono essere configurati con un accesso più restrittivo. I criteri di gruppo restrittivi devono consentire esplicitamente a ogni azione di cui si desidera che gli utenti o l'applicazione siano in grado di eseguire e negare esplicitamente le azioni di cui non si desidera che siano in grado di eseguire tali azioni. NetApp sconsiglia l'utilizzo di un'opzione con caratteri jolly, poiché in futuro potrebbe essere introdotta una nuova azione e si desidera controllare se è consentita o negata. Per questa soluzione, l'elenco di negazione deve includere DeleteObjectVersion, PutBucketPolicy, DeleteBucketPolicy, PutLifecycleConfiguration e PutBucketVersioning per proteggere la configurazione delle versioni del bucket e delle versioni dell'oggetto da modifiche dell'utente o del programma.

In StorageGRID l'opzione del criterio di gruppo S3 "Mitigazione ransomware" semplifica l'implementazione di questa soluzione. Quando si crea un gruppo di utenti nel tenant, dopo aver selezionato le autorizzazioni del gruppo, è possibile visualizzare questa policy facoltativa.



Di seguito viene riportato il contenuto dei criteri di gruppo che includono la maggior parte delle operazioni disponibili esplicitamente consentite e il minimo richiesto negato.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteReplicationConfiguration",
```

```
"s3:DeleteBucketMetadataNotification",
                "s3:GetBucketAcl",
                "s3:GetBucketCompliance",
                "s3:GetBucketConsistency",
                "s3:GetBucketLastAccessTime",
                "s3:GetBucketLocation",
                "s3:GetBucketNotification"
"s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicy",
                "s3:GetBucketMetadataNotification",
                "s3:GetReplicationConfiguration",
                "s3:GetBucketCORS",
                "s3:GetBucketVersioning",
                "s3:GetBucketTagging",
                "s3:GetEncryptionConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:ListAllMyBuckets",
                "s3:ListBucketMultipartUploads",
                "s3:PutBucketConsistency",
                "s3:PutBucketLastAccessTime",
                "s3:PutBucketNotification",
"s3:PutBucketObjectLockConfiguration",
                "s3:PutReplicationConfiguration",
                "s3:PutBucketCORS",
                "s3:PutBucketMetadataNotification",
                "s3:PutBucketTagging",
                "s3:PutEncryptionConfiguration",
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersionTagging",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectVersionTagging",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectLegalHold",
                "s3:PutObjectRetention",
```

```
                "s3:PutObjectTagging",
                "s3:PutObjectVersionTagging",
                "s3:RestoreObject",
                "s3:ValidateObject",
                "s3:PutBucketCompliance",
                "s3:PutObjectVersionAcl"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "s3:DeleteObjectVersion",
                "s3:DeleteBucketPolicy",
                "s3:PutBucketPolicy",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketVersioning"
            ],
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

Indagine e bonifica del ransomware

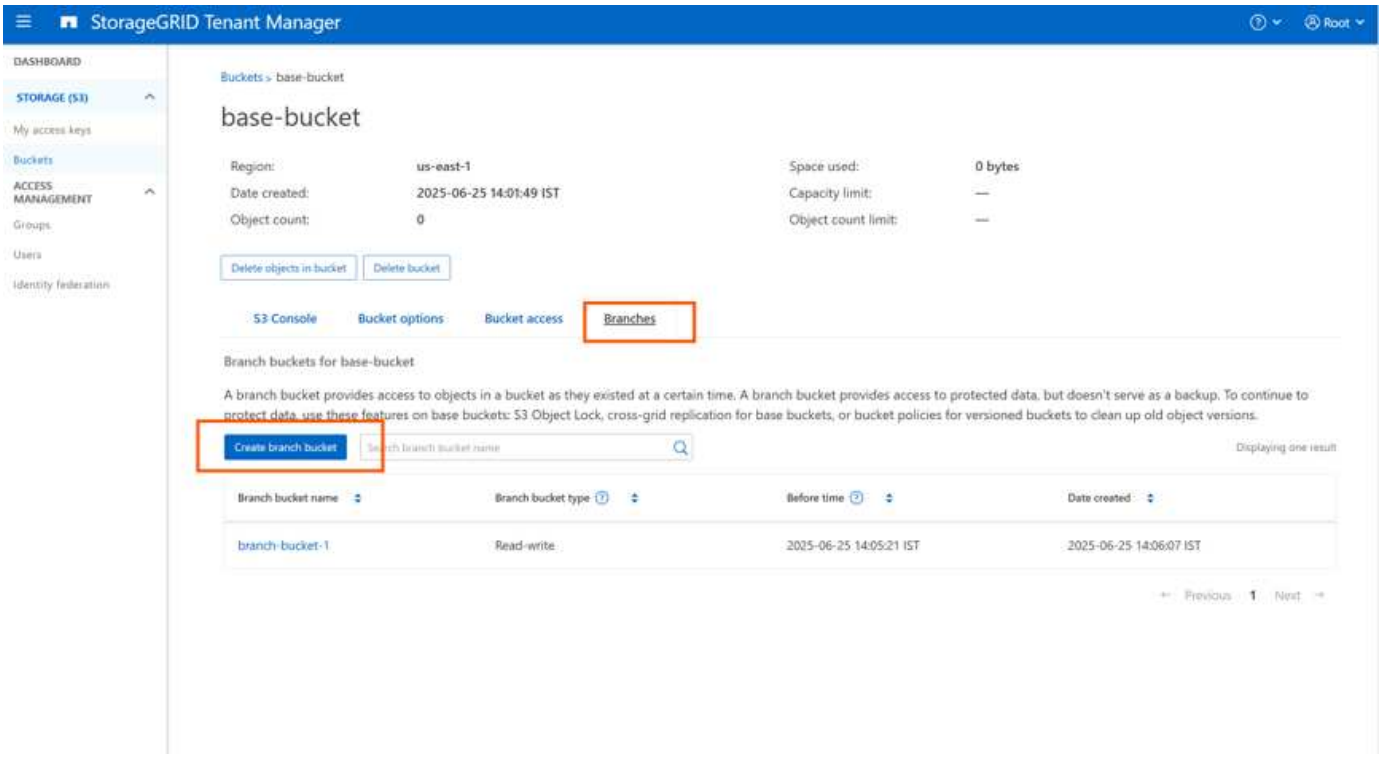
Scopri come analizzare e correggere i bucket dopo un possibile attacco ransomware con StorageGRID.

In StorageGRID 12.0 è stata aggiunta la nuova funzionalità branch bucket per ampliare l'utilità del controllo delle versioni per la difesa dal ransomware. Un bucket di diramazione fornisce l'accesso agli oggetti in un bucket così come esistevano in un determinato momento, a condizione che siano ancora presenti nel bucket. I bucket di diramazione possono essere creati solo per i bucket di base abilitati al controllo delle versioni.

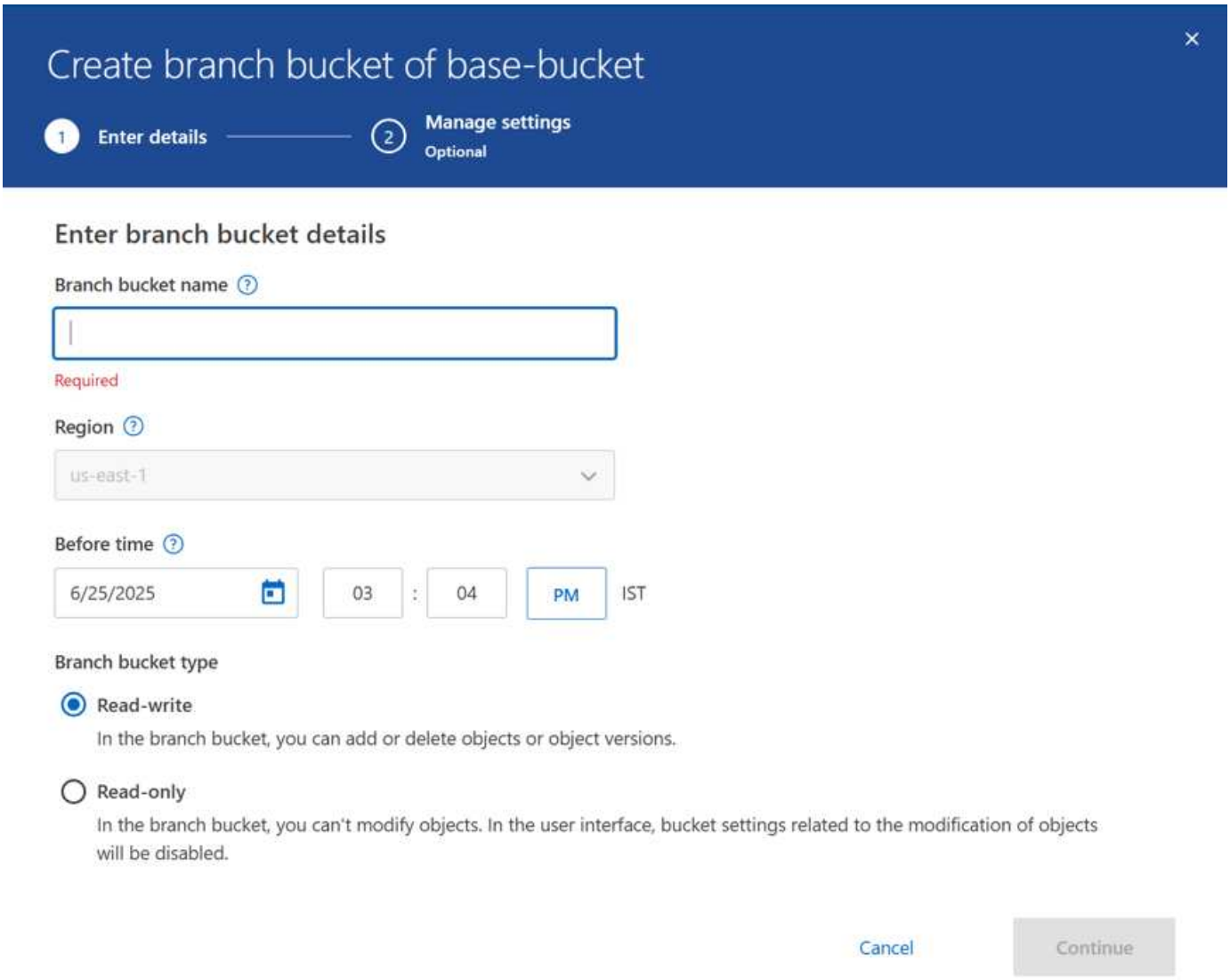
Ciò significa che se sospetti che si sia verificato un attacco ransomware, puoi creare un bucket di ramificazione di lettura/scrittura o di sola lettura contenente tutti gli oggetti e le versioni esistenti prima dell'attacco iniziale. È possibile utilizzare questo bucket di diramazione per effettuare un confronto con il contenuto del bucket di base, per scoprire quali oggetti sono cambiati e se la modifica faceva parte dell'attacco o meno. È anche possibile utilizzare un branch bucket per continuare le operazioni del client utilizzando il branch pulito mentre si indaga sull'attacco.

Creazione di un bucket Branch

- Passare alla pagina dei dettagli del bucket di base e alla scheda Branch per creare un bucket branch.



- Dopo aver cliccato sul pulsante Crea bucket di diramazione, si aprirà una finestra popup con i dettagli precompilati della regione associata al bucket di base.
- fornire il nome del bucket di diramazione, prima dell'ora, e selezionare il tipo di bucket di diramazione da creare.



TR-4765: StorageGRID monitor

Introduzione al monitoraggio StorageGRID

Scopri come monitorare il tuo sistema StorageGRID utilizzando applicazioni esterne, come Splunk.

Un efficace monitoraggio dello storage basato su oggetti NetApp StorageGRID permette agli amministratori di rispondere rapidamente ai problemi urgenti e di aggiungere risorse in modo proattivo per gestire carichi di lavoro in crescita. Questo report fornisce una guida generale su come monitorare le metriche chiave e come sfruttare le applicazioni di monitoraggio esterne. Lo scopo è di integrare la guida al monitoraggio e alla risoluzione dei problemi esistente.

Un'implementazione NetApp StorageGRID è costituita generalmente da diversi siti e nodi che operano per creare un sistema di storage a oggetti distribuito e tollerante agli errori. In un sistema storage distribuito e resiliente come StorageGRID, è normale che sussistano condizioni di errore mentre il grid continua a funzionare normalmente. La sfida per l'amministratore è capire la soglia alla quale le condizioni di errore (come i nodi inattivi) presentano un problema che deve essere immediatamente affrontato rispetto alle informazioni che devono essere analizzate. Analizzando i dati presenti in StorageGRID, potrai comprendere il tuo carico di

lavoro e prendere decisioni informate, come ad esempio quando aggiungere altre risorse.

StorageGRID fornisce un'eccellente documentazione che approfondisce l'argomento del monitoraggio. Questo report presuppone che l'utente abbia acquisito dimestichezza con StorageGRID e che abbia esaminato la relativa documentazione. Invece di ripetere queste informazioni, in questa guida si fa riferimento alla documentazione del prodotto. La documentazione dei prodotti StorageGRID è disponibile online e in formato PDF.

L'obiettivo di questo documento è integrare la documentazione di prodotto e discutere delle modalità di monitoraggio del sistema StorageGRID utilizzando applicazioni esterne come Splunk.

Origini dei dati

Per monitorare con successo NetApp StorageGRID, è importante sapere dove raccogliere dati sullo stato e sul funzionamento del sistema StorageGRID.

- **Interfaccia utente Web e dashboard.** Il gestore di griglie StorageGRID presenta una vista di livello superiore delle informazioni che l'amministratore deve visualizzare in una presentazione logica. Gli amministratori possono inoltre approfondire le informazioni sul livello di servizio per la risoluzione dei problemi e la raccolta di log.
- **Registri di controllo.** StorageGRID mantiene registri di audit granulari delle azioni dei tenant come PUT, GET ed DELETE. È anche possibile tracciare il ciclo di vita di un oggetto, dall'acquisizione all'applicazione di regole di gestione dei dati.
- **API metriche.** Alla base dell'interfaccia GMI di StorageGRID vi sono API aperte, in quanto l'interfaccia utente è basata su API. Questo approccio consente di estrarre i dati utilizzando strumenti esterni di analisi e monitoring.

Dove trovare ulteriori informazioni

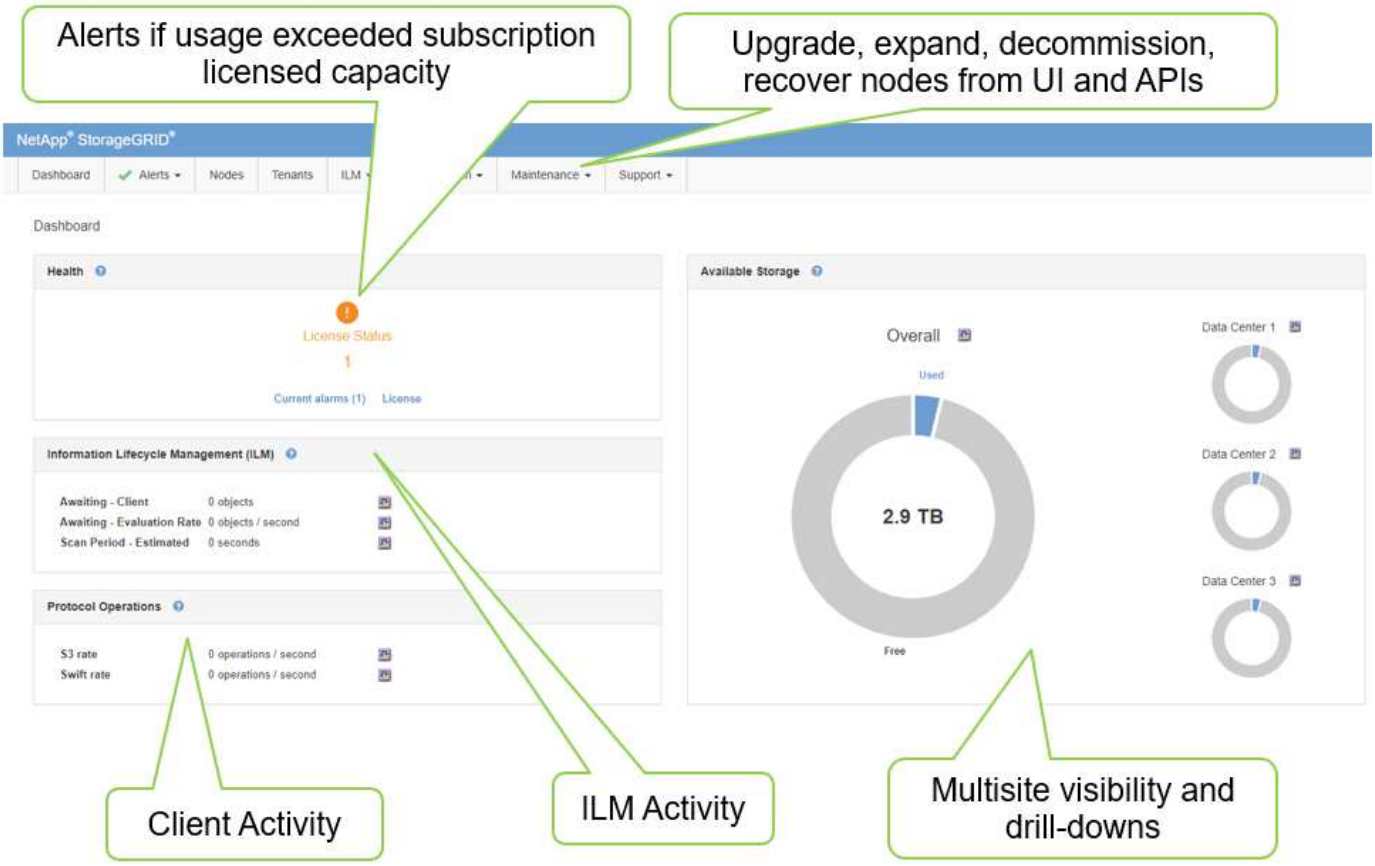
Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti e/o siti Web:

- Centro di documentazione NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-118/
- Abilitazione NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Documentazione dei prodotti NetApp https://www.netapp.com/support-and-training/documentation/
- App NetApp StorageGRID per Splunk https://splunkbase.splunk.com/app/3898/#/details

Utilizzare il dashboard GMI per monitorare StorageGRID

La dashboard dell'interfaccia GMI (Grid Management Interface) di StorageGRID fornisce una vista centralizzata dell'infrastruttura StorageGRID, consentendo di controllare lo stato, le prestazioni e la capacità dell'intero grid.

Utilizzare il dashboard GMI per esaminare ciascun componente principale della griglia.



Informazioni che è necessario monitorare regolarmente

In una versione precedente di questo report tecnico sono elencate le metriche da controllare periodicamente rispetto alle tendenze. Tali informazioni sono ora incluse nella "Guida al monitoraggio e alla risoluzione di problemi".

Monitoraggio dei costi

Una versione precedente di questo report tecnico elenca le aree in cui monitorare metriche importanti, come Object Storage Space, Metadata Space, Network Resources e così via. Tali informazioni sono ora incluse nella "Guida al monitoraggio e alla risoluzione di problemi".

Utilizzare gli avvisi per monitorare StorageGRID

Informazioni su come utilizzare il sistema di avvisi in StorageGRID per monitorare i problemi, gestire avvisi personalizzati ed estendere le notifiche di avviso tramite SNMP o e-mail.

Gli avvisi forniscono informazioni critiche che consentono di monitorare i vari eventi e condizioni all'interno del sistema StorageGRID.

Il sistema di avvisi è progettato per essere lo strumento principale per il monitoraggio di eventuali problemi che potrebbero verificarsi nel sistema StorageGRID. Il sistema di avvisi è incentrato su problemi pratici nel sistema e offre un'interfaccia semplice da utilizzare.

Forniamo una varietà di regole di avviso predefinite che mirano a monitorare e risolvere i problemi del sistema. È possibile gestire ulteriormente gli avvisi creando avvisi personalizzati, modificando o disabilitando gli avvisi

predefiniti e tacitando le notifiche degli avvisi.

È possibile estendere gli avvisi anche tramite notifiche SNMP o e-mail.

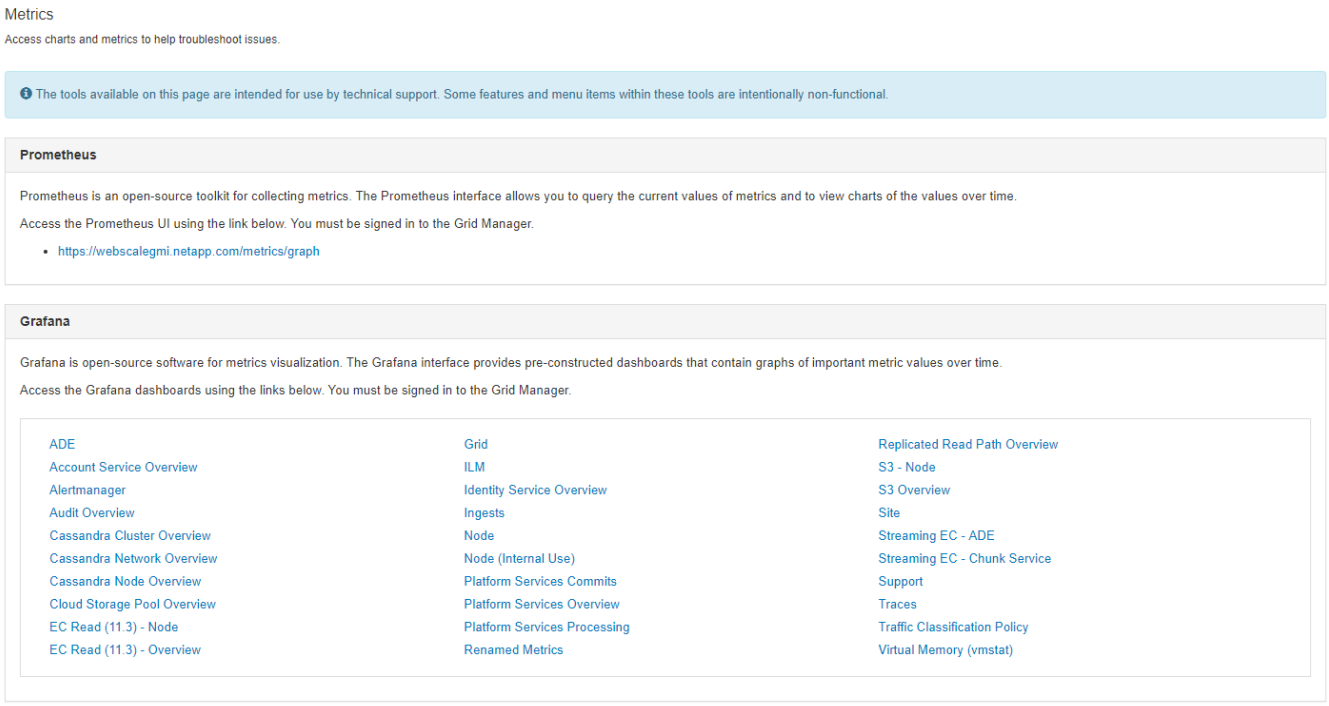
Per ulteriori informazioni sugli avvisi, vedere la "documentazione del prodotto" disponibile online e in formato PDF.

Monitoraggio avanzato in StorageGRID

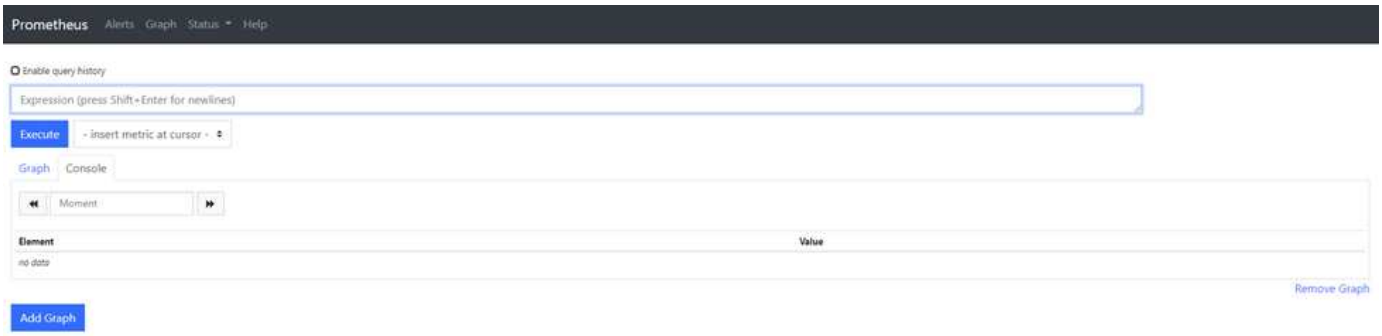
Scopri come accedere ed esportare le metriche per risolvere i problemi.

Visualizzare l'API delle metriche tramite una query Prometheus

Prometheus è un software open-source per la raccolta delle metriche. Per accedere al Prometheus integrato di StorageGRID tramite l'GMI, vai al **Support › Metrics**.



In alternativa, è possibile accedere direttamente al collegamento.

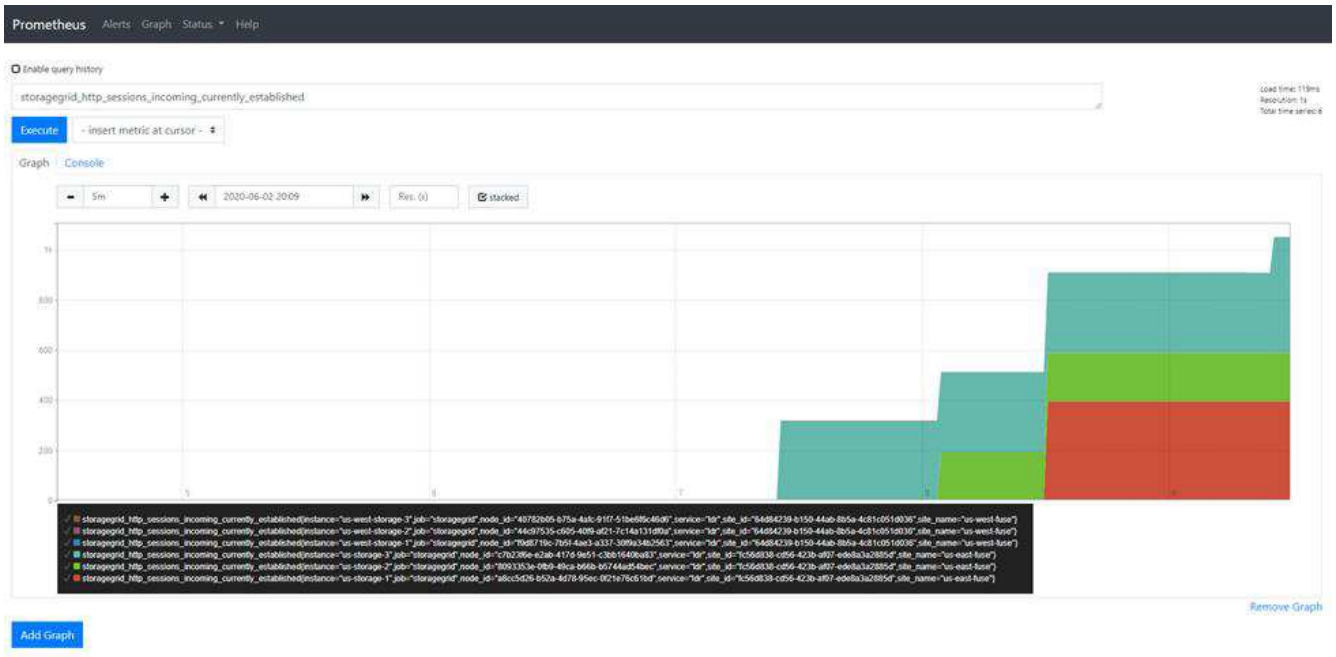


Con questa visualizzazione, è possibile accedere all'interfaccia Prometheus. Da lì, puoi cercare nelle metriche disponibili e persino sperimentare le query.

Per eseguire una query URL Prometheus, attenersi alla seguente procedura:

Fasi

1. Iniziare a digitare nella casella di testo della query. Durante la digitazione, vengono elencate le metriche. Per i nostri scopi, sono importanti solo le metriche che iniziano con StorageGRID e nodo.
2. Per visualizzare il numero di sessioni HTTP per ogni nodo, digitare `storagegrid_http` e selezionare `storagegrid_http_sessions_incoming_currently_established`. Fare clic su Esegui e visualizzare le informazioni in formato grafico o console.



Le query e i grafici creati tramite questo URL non persistono. Le query complesse consumano risorse sul nodo amministrativo. NetApp consiglia di utilizzare questa vista per esplorare le metriche disponibili.

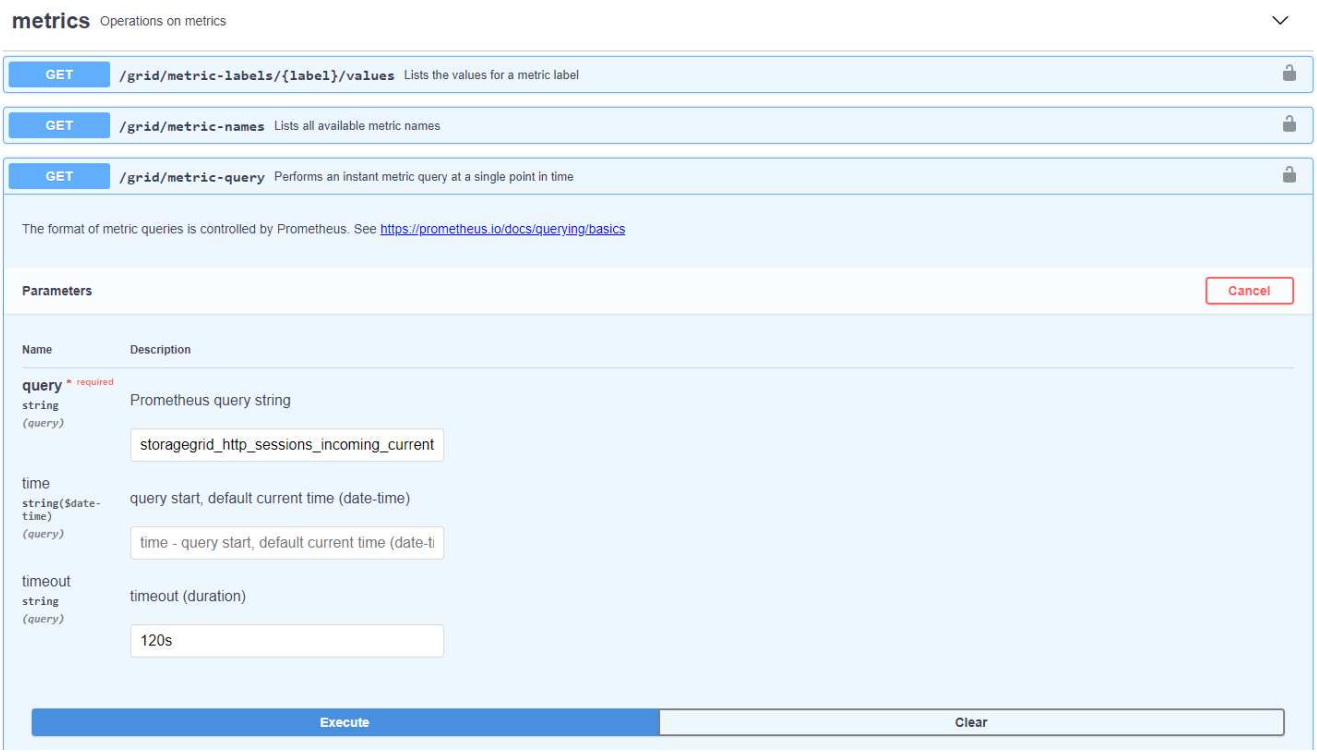
Si sconsiglia di interfacciarsi direttamente con la nostra istanza Prometheus perché questo richiede l'apertura di porte aggiuntive. L'accesso alle metriche tramite la nostra API è il metodo consigliato e sicuro.

Esporta metriche tramite API

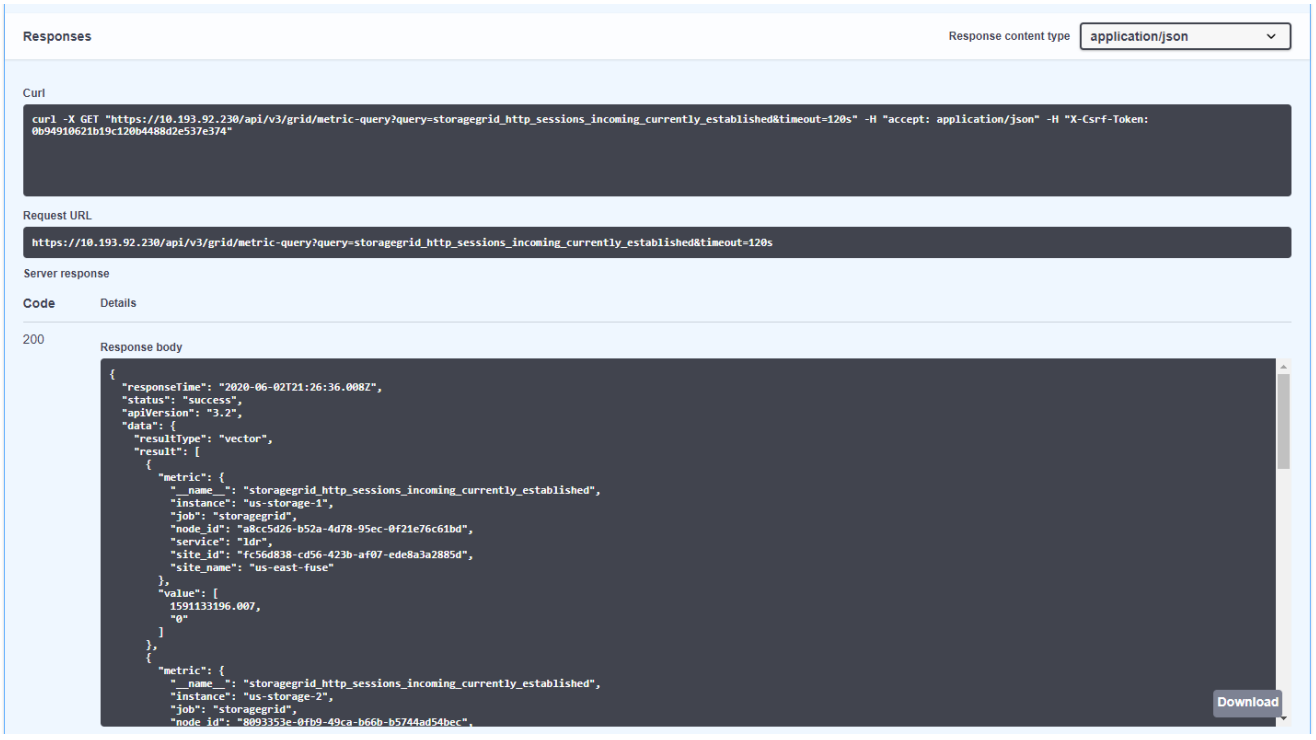
Puoi anche accedere agli stessi dati tramite l'API di gestione StorageGRID.

Per esportare le metriche tramite l'API, attenersi alla seguente procedura:

1. Nell'interfaccia GMI, selezionare **Guida › documentazione API**.
2. Scorrere fino a Metrics (metriche) e selezionare GET /grid/METRIC-query (OTTIENI /griglia/query metrica).



La risposta include le stesse informazioni che è possibile ottenere tramite una query URL Prometheus. È possibile visualizzare nuovamente il numero di sessioni HTTP attualmente stabilite su ciascun nodo di storage. È anche possibile scaricare la risposta in formato JSON per la leggibilità. La figura seguente mostra risposte di query Prometheus di esempio.



Il vantaggio dell'utilizzo dell'API è che consente di eseguire query autenticate

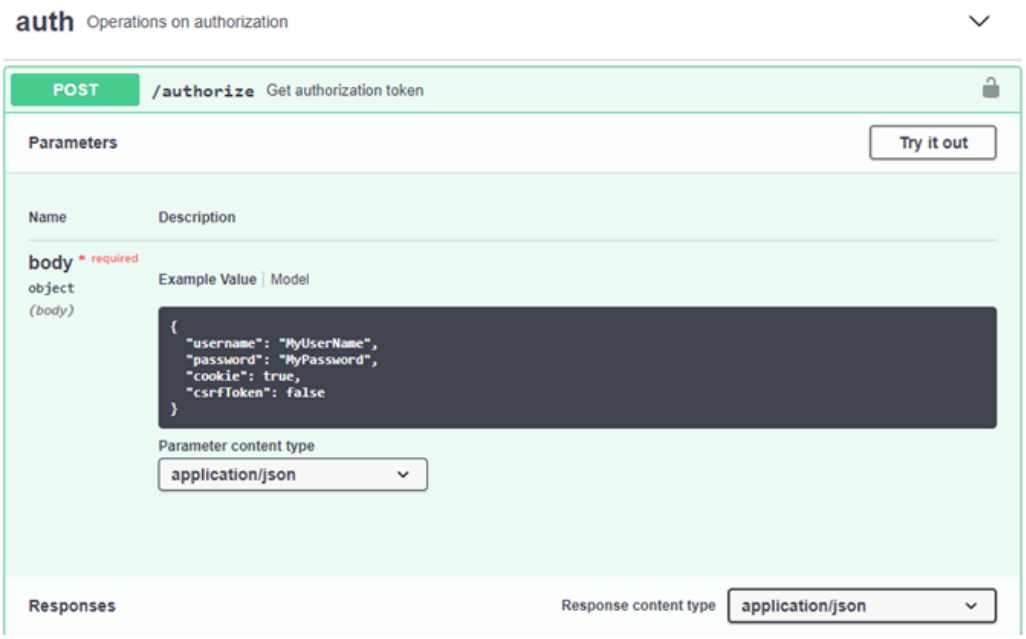
Accedi alle metriche utilizzando Curl in StorageGRID

Scopri come accedere alle metriche tramite l'interfaccia CLI utilizzando Curl.

Per eseguire questa operazione, è necessario prima ottenere un token di autorizzazione. Per richiedere un token, attenersi alla seguente procedura:

Fasi

1. Nell'interfaccia GMI, selezionare **Guida › documentazione API**.
2. Scorrere verso il basso fino a Auth per trovare le operazioni su autorizzazione. La seguente schermata mostra i parametri per il metodo POST.



3. Fare clic su prova e modificare il corpo con il nome utente e la password GMI.
4. Fare clic su Esegui.
5. Copiare il comando curl fornito nella sezione curl e incollarlo in una finestra terminale. Il comando è simile al seguente:

```
curl -X POST "https:// <Primary_Admin_IP>/api/v3/authorize" -H "accept:
application/json" -H "Content-Type: application/json" -H "X-Csrf-Token:
dc30b080e1ca9bc05ddb81104381d8c8" -d "{ \"username\": \"MyUsername\",
\"password\": \"MyPassword\", \"cookie\": true, \"csrfToken\": false}"
-k
```

> Se la password GMI contiene caratteri speciali, utilizzare \ per uscire da caratteri speciali. Ad esempio, sostituire ! con \!

6. Dopo aver eseguito il comando curl precedente, l'output fornisce un token di autorizzazione come l'esempio seguente:

```
{"responseTime":"2020-06-
03T00:12:17.031Z","status":"success","apiVersion":"3.2","data":"8a1e528d
-18a7-4283-9a5e-b2e6d731e0b2"}
```

Ora è possibile utilizzare la stringa del token di autorizzazione per accedere alle metriche tramite curl. Il processo di accesso alle metriche è simile a quello descritto nella sezione "Monitoraggio avanzato in StorageGRID". Tuttavia, a scopo dimostrativo, viene mostrato un esempio con GET /grid/metric-labels/{label}/values selezionato nella categoria Metrics.

7. Ad esempio, il seguente comando curl con il token di autorizzazione precedente elenca i nomi dei siti in StorageGRID.

```
curl -X GET "https://10.193.92.230/api/v3/grid/metric-
labels/site_name/values" -H "accept: application/json" -H
"Authorization: Bearer 8a1e528d-18a7-4283-9a5e-b2e6d731e0b2"
```

Il comando curl genera il seguente output:

```
{"responseTime":"2020-06-
03T00:17:00.844Z","status":"success","apiVersion":"3.2","data":["us-
east-fuse","us-west-fuse"]}
```

Visualizza le metriche utilizzando la dashboard Grafana di StorageGRID

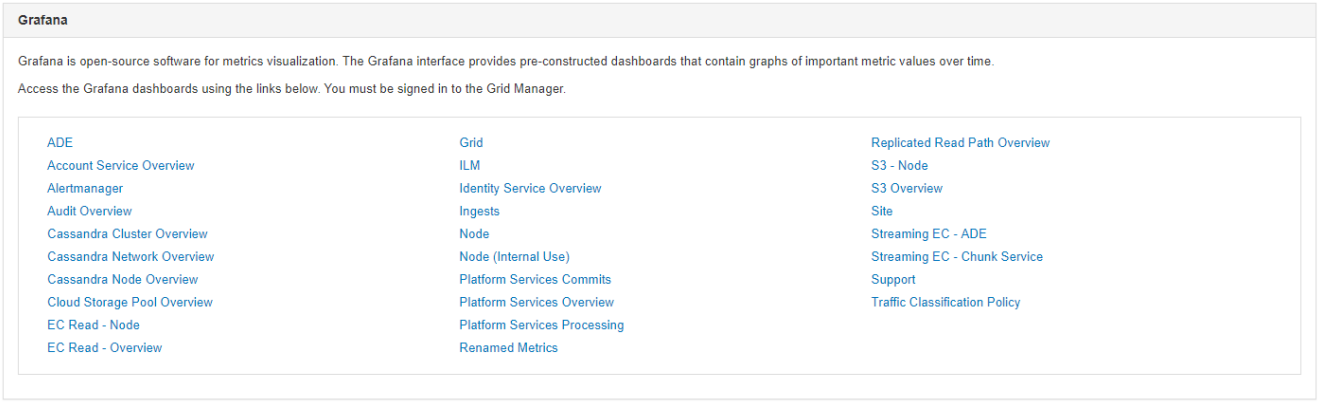
Scopri come utilizzare l'interfaccia Grafana per visualizzare e monitorare i tuoi dati StorageGRID.

Grafana è un software open-source per la visualizzazione delle metriche. Per impostazione predefinita, sono disponibili dashboard predefiniti che forniscono informazioni utili e potenti sul sistema StorageGRID in uso.

Questi dashboard predefiniti sono utili non solo per il monitoraggio ma anche per la risoluzione di un problema. Alcune sono destinate all'uso da parte del supporto tecnico. Ad esempio, per visualizzare le metriche di un nodo storage, segui questa procedura.

Fasi

1. Nell'interfaccia GMI, **Support › Metrics** (supporto[metriche]).
2. Nella sezione Grafana, selezionare il dashboard Node (nodo).



3. In Grafana, impostare gli host sul nodo su cui si desidera visualizzare le metriche. In questo caso, viene selezionato un nodo storage. Vengono fornite ulteriori informazioni rispetto alle seguenti schermate acquisite.

Utilizzare i criteri di classificazione del traffico in StorageGRID

Scoprite come impostare e configurare criteri di classificazione del traffico per gestire e ottimizzare il traffico di rete in StorageGRID.

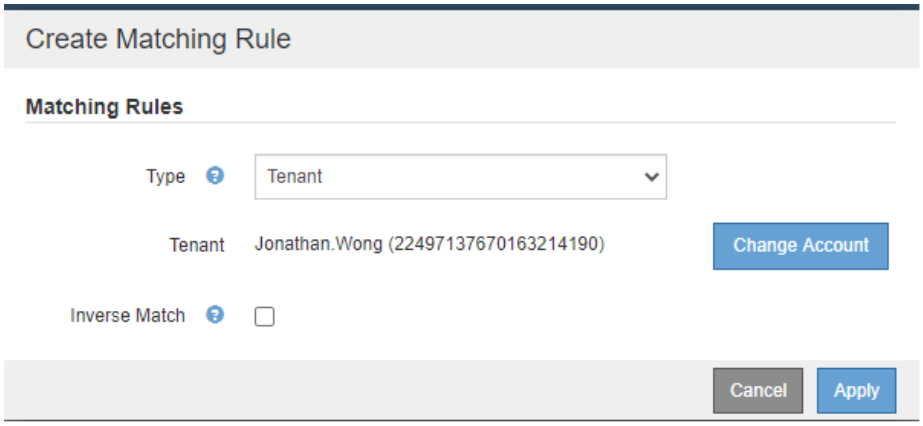
I criteri di classificazione del traffico forniscono un metodo per monitorare e/o limitare il traffico in base a specifici endpoint di tenant, bucket, subnet IP o bilanciamento del carico. La connettività di rete e la larghezza di banda sono parametri particolarmente importanti per StorageGRID.

Per configurare un criterio di classificazione del traffico, attenersi alla seguente procedura:

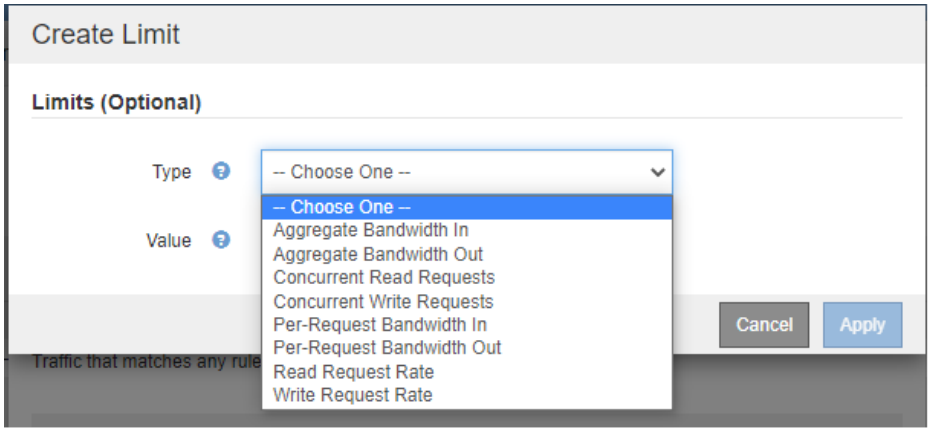
Fasi

1. Sull'interfaccia GMI, accedere al **Configurazione › Impostazioni del sistema › classificazione del traffico**.
2. Fare clic su Crea +

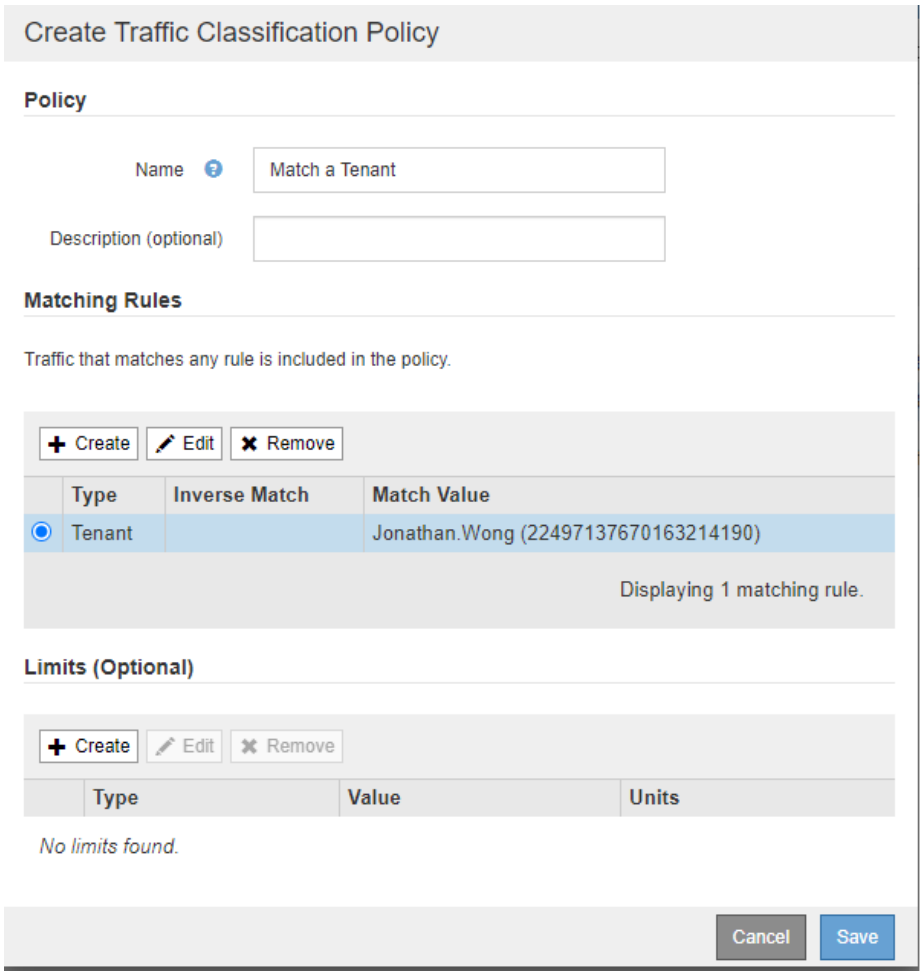
3. Immettere un nome e una descrizione per la politica.
4. Creare una regola corrispondente.



5. Impostare un limite (opzionale).



6. Salvare la policy



Per visualizzare le metriche associate al criterio di classificazione del traffico, selezionare il criterio e fare clic su metriche. Viene generata una dashboard Grafana che visualizza informazioni come il traffico delle richieste di bilanciamento del carico e la durata media delle richieste.

Utilizzare i registri di controllo per monitorare StorageGRID

Scopri come utilizzare l'audit log di StorageGRID per approfondimenti dettagliati sulle attività di tenant e grid e come sfruttare strumenti come Splunk per l'analisi dei log.

L'audit log di StorageGRID consente di raccogliere informazioni dettagliate sul tenant e sull'attività della griglia. L'audit log può essere esposto per analisi tramite NFS. Per istruzioni dettagliate su come esportare il registro di controllo, consultare la Guida dell'amministratore.

Dopo l'esportazione della audit, puoi utilizzare strumenti di analisi dei log come Splunk o Logstash + Elasticsearch per comprendere l'attività dei tenant o creare report dettagliati su fatturazione e charge back.

I dettagli sui messaggi di controllo sono inclusi nella documentazione di StorageGRID. Vedere "Messaggi di audit".

USA l'app StorageGRID per Splunk

Scopri l'app NetApp StorageGRID per Splunk, che consente di monitorare e analizzare il tuo ambiente StorageGRID all'interno della piattaforma Splunk.

Splunk è una piattaforma software che importa e indicizza i dati delle macchine per fornire potenti funzionalità di ricerca e analisi. L'app NetApp StorageGRID è un add-on per Splunk che importa e arricchisce i dati sfruttati da StorageGRID.

Le istruzioni su come installare, aggiornare e configurare il componente aggiuntivo StorageGRID sono disponibili qui: https://splunkbase.splunk.com/app/3895/#/details

TR-4882: Installazione di una griglia bare metal StorageGRID

Introduzione all'installazione di StorageGRID

Scopri come installare StorageGRID su host bare metal.

TR-4882 fornisce una pratica serie di istruzioni passo-passo che produce un'installazione funzionante di NetApp StorageGRID. L'installazione potrebbe essere su server bare metal o su macchine virtuali (VM) in esecuzione su Red Hat Enterprise Linux (RHEL). L'approccio consiste nell'eseguire un'installazione "chiavi in mano" di sei servizi racchiusi in container StorageGRID su tre macchine fisiche (o virtuali), seguendo un layout e una configurazione dello storage suggeriti. Per alcuni clienti potrebbe essere più semplice comprendere il processo di implementazione, seguire l'esempio riportato in questo report tecnico.

Per una comprensione più approfondita di StorageGRID e del processo di installazione, vedere https://docs.netapp.com/us-en/storagegrid-118/landing-install-upgrade/index.html [Installazione, aggiornamento e aggiornamento rapido StorageGRID] nella documentazione del prodotto.

Prima di iniziare l'implementazione, esaminiamo i requisiti di calcolo, storage e rete per il software NetApp StorageGRID. StorageGRID viene eseguito come servizio containerizzato all'interno di Podman o Docker. In questo modello, alcuni requisiti fanno riferimento al sistema operativo host (il sistema operativo che ospita Docker, che esegue il software StorageGRID). Inoltre, alcune risorse vengono allocate direttamente nei container Docker eseguiti all'interno di ciascun host. In questa distribuzione, al fine di ottimizzare l'utilizzo dell'hardware, vengono distribuiti due servizi per host fisico. Per ulteriori informazioni, passare alla sezione successiva, "Prerequisiti per l'installazione di StorageGRID".

I passaggi descritti in questo TR comportano un'installazione StorageGRID funzionante su sei host bare metal. Ora si dispone di una griglia di lavoro e di una rete client, utili nella maggior parte degli scenari di test.

Dove trovare ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo report tecnico, consultare le seguenti risorse della documentazione:

- Centro di documentazione NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-118/
- Abilitazione NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Documentazione dei prodotti NetApp https://www.netapp.com/support-and-training/documentation/

Prerequisiti per l'installazione di StorageGRID

Scopri i requisiti di calcolo, storage, rete, docker e nodo per implementare StorageGRID.

Requisiti di calcolo

La tabella riportata di seguito elenca i requisiti minimi delle risorse supportate per ogni tipo di nodo StorageGRID. Queste sono le risorse minime richieste per i nodi StorageGRID.

Tipo di nodo	Core di CPU	RAM
Amministratore	8	24GB
Storage	8	24GB
Gateway	8	24GB

Inoltre, per garantire il corretto funzionamento di ciascun host fisico di Docker deve essere allocato un minimo di 16GB GB di RAM. Ad esempio, per ospitare insieme due dei servizi descritti nella tabella in un unico host fisico di Docker, occorre eseguire il seguente calcolo:

24 + 24 + 16 = 64GB GB di RAM e 8 + 8 = 16 core

Poiché molti server moderni superano questi requisiti, combiniamo sei servizi (container StorageGRID) su tre server fisici.

Requisiti di rete

I tre tipi di traffico StorageGRID includono:

- **Traffico griglia (obbligatorio).** Il traffico StorageGRID interno che viaggia tra tutti i nodi della griglia.
- **Traffico amministrativo (opzionale).** Il traffico utilizzato per l'amministrazione e la manutenzione del sistema.
- **Traffico client (opzionale).** Il traffico che viaggia tra le applicazioni client esterne e il grid, incluse tutte le richieste di storage a oggetti dai client S3 e Swift.

È possibile configurare fino a tre reti da utilizzare con il sistema StorageGRID. Ogni tipo di rete deve trovarsi su una subnet separata senza sovrapposizioni. Se tutti i nodi si trovano nella stessa subnet, non è necessario un indirizzo gateway.

Per questa valutazione, verrà eseguita la distribuzione su due reti, che contengono la rete e il traffico client. È

possibile aggiungere successivamente una rete di amministrazione per supportare questa funzione aggiuntiva.

È molto importante mappare le reti in modo coerente alle interfacce in tutti gli host. Ad esempio, se su ogni nodo sono presenti due interfacce, ens192 e ens224, tutte devono essere mappate alla stessa rete o VLAN su tutti gli host. In questa installazione, il programma di installazione esegue il mapping di questi dati nei contenitori Docker come eth0@IF2 e eth2@IF3 (poiché il loopback è IF1 all'interno del contenitore), pertanto un modello coerente è molto importante.

Nota sul networking di Docker

StorageGRID utilizza il networking in modo diverso da alcune implementazioni di container Docker. Non utilizza il networking fornito da Docker (o Kubernetes o Swarm). Al contrario, in realtà StorageGRID utilizza il container come --net=none, in modo che Docker non esegua alcuna operazione di rete. Dopo che il contenitore è stato generato dal servizio StorageGRID, viene creato un nuovo dispositivo macvlan dall'interfaccia definita nel file di configurazione del nodo. Tale dispositivo dispone di un nuovo indirizzo MAC e funge da dispositivo di rete separato in grado di ricevere pacchetti dall'interfaccia fisica. Il dispositivo macvlan viene quindi spostato nello spazio dei nomi dei contenitori e rinominato in uno dei eth0, eth1 o eth2 all'interno del contenitore. A questo punto, il dispositivo di rete non è più visibile nel sistema operativo host. Nel nostro esempio, il dispositivo di rete Grid è eth0 all'interno dei container Docker e la rete Client è eth2. Se avessimo una rete di amministrazione, il dispositivo sarebbe eth1 nel container.

> Il nuovo indirizzo MAC del dispositivo di rete del contenitore potrebbe richiedere l'attivazione della modalità promiscua in alcuni ambienti di rete e virtuali. Questa modalità consente al dispositivo fisico di ricevere e inviare pacchetti per gli indirizzi MAC che differiscono dagli indirizzi MAC fisici noti. se si esegue in VMware vSphere, è necessario accettare la modalità promiscua, le modifiche degli indirizzi MAC e le trasmissioni falsificate nei gruppi di porte che serviranno il traffico StorageGRID quando si esegue RHEL. Ubuntu o Debian funziona senza questi cambiamenti nella maggior parte delle circostanze.

Requisiti di storage

I nodi richiedono ciascuno dispositivi di dischi locali o basati su SAN delle dimensioni indicate nella tabella seguente.

> I numeri contenuti nella tabella sono relativi a ciascun tipo di servizio StorageGRID, non all'intero grid o a ciascun host fisico. In base alle scelte di distribuzione, verranno calcolati i numeri per ciascun host fisico in , più avanti in "Layout e requisiti dell'host fisico"questo documento. i percorsi o i file system contrassegnati con un asterisco verranno creati nel contenitore StorageGRID stesso dall'installatore. L'amministratore non richiede alcuna configurazione manuale o creazione di file system, ma gli host hanno bisogno di dispositivi a blocchi per soddisfare questi requisiti. In altre parole, il dispositivo a blocchi dovrebbe apparire utilizzando il comando `lsblk` ma non essere formattato o montato all'interno del sistema operativo host.

Tipo di nodo	Scopo del LUN	Numero di LUN	Dimensione minima di LUN	File system manuale richiesto	Voce di configurazione nodo consigliata
Tutto	Spazio di sistema del nodo amministrativo `/var/local` (SSD utile qui)	Uno per ogni nodo amministrativo	90GB	No	`BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/ADM-VAR-LOCAL`

Tipo di nodo	Scopo del LUN	Numero di LUN	Dimensione minima di LUN	File system manuale richiesto	Voce di configurazione nodo consigliata
Tutti i nodi	Pool di storage Docker all'indirizzo `/var/lib/docker for container pool`	Uno per ciascun host (fisico o VM)	100GB per contenitore	Sì – etx4	NA – formatta e monta come file system host (non mappato nel contenitore)
Amministratore	Audit log del nodo amministrativo (dati del sistema nel container dell'amministratore) `/var/local/audit/export`	Uno per ogni nodo amministrativo	200GB	No	`BLOCK_DEVICE_AUDIT_LOGS =/dev/mapper/ADM-OS`
Amministratore	Tabelle nodo amministrativo (dati di sistema nel contenitore amministrativo) `/var/local/mysql_ibdata`	Uno per ogni nodo amministrativo	200GB	No	`BLOCK_DEVICE_TABLES = /dev/mapper/ADM-MySQL`
Nodi di storage	Storage a oggetti (dispositivi a blocchi `/var/local/rangedb0`) (SSD utili qui) `/var/local/rangedb1` `/var/local/rangedb2`	Tre per ciascun contenitore di stoccaggio	4000GB	No	`BLOCK_DEVICE_RANGEDB_000 = /dev/mapper/SN-Db00` `BLOCK_DEVICE_RANGEDB_001 = /dev/mapper/SN-Db01` `BLOCK_DEVICE_RANGEDB_002 = /dev/mapper/SN-Db02`

In questo esempio, le dimensioni dei dischi mostrate nella seguente tabella sono necessarie per tipo di contenitore. I requisiti per host fisico sono descritti nella , più avanti in "Layout e requisiti dell'host fisico"questo documento.

Dimensioni dei dischi per tipo di container

Container di amministrazione

Nome	Dimensioni (GiB)
Docker-Store	100 (per contenitore)
ADM-OS	90
ADM-Audit	200
ADM-MySQL	200

Contenitore di stoccaggio

Nome	Dimensioni (GiB)
Docker-Store	100 (per contenitore)
SN-OS	90
Rangedb-0	4096
Rangedb-1	4096
Rangedb-2	4096

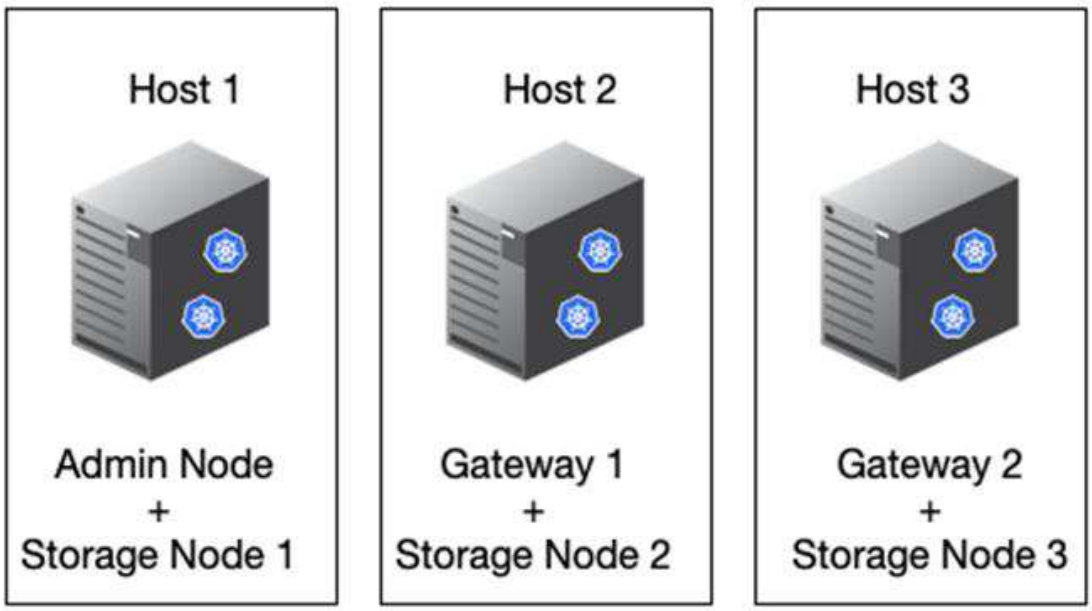
Contenitore gateway

Nome	Dimensioni (GiB)
Docker-Store	100 (per contenitore)
/var/local	90

Layout e requisiti dell'host fisico

Combinando i requisiti di elaborazione e di rete illustrati nella tabella precedente, è possibile ottenere un set di hardware di base necessario per questa installazione di tre server fisici (o virtuali) con 16 core, 64GB di RAM e due interfacce di rete. Se si desidera un throughput più elevato, è possibile collegare due o più interfacce sulla griglia o sulla rete client e utilizzare un'interfaccia con codifica VLAN come bond0,520 nel file di configurazione del nodo. In presenza di carichi di lavoro più intensi, è preferibile una maggiore quantità di memoria per l'host e i container.

Come illustrato nella seguente figura, questi server ospitano sei container Docker, due per host. La RAM viene calcolata fornendo 24GB GB per contenitore e 16GB GB per il sistema operativo host stesso.



La RAM totale richiesta per host fisico (o VM) è 24 x 2 GB + 16 GB = 64GB GB. Nelle tabelle che seguono sono elencati i requisiti di archiviazione su disco per gli host 1, 2 e 3.

Host 1	**Dimensioni (GiB)**
Docker Store	`/var/lib/docker` (File system)
200 (100 x 2)	**Contenitore amministratore**
`BLOCK_DEVICE_VAR_LOCAL`	90
`BLOCK_DEVICE_AUDIT_LOGS`	200
`BLOCK_DEVICE_TABLES`	200
Contenitore di stoccaggio	SN-OS `/var/local` (dispositivo)
90	Rangedb-0 (dispositivo)
4096	Rangedb-1 (dispositivo)
4096	Rangedb-2 (dispositivo)

Host 2	**Dimensioni (GiB)**
Docker Store	`/var/lib/docker` (Condiviso)
200 (100 x 2)	**Contenitore gateway**
GW-OS */var/local	100
Contenitore di stoccaggio	*/var/local
100	Rangedb-0
4096	Rangedb-1
4096	Rangedb-2

Host 3	**Dimensioni (GiB)**
Docker Store	`/var/lib/docker` (Condiviso)
200 (100 x 2)	**Contenitore gateway**
*/var/local	100
Contenitore di stoccaggio	*/var/local
100	Rangedb-0
4096	Rangedb-1
4096	Rangedb-2

Docker Store è stato calcolato consentendo 100GB per /var/local (per contenitore) x due contenitori = 200GB.

Preparazione dei nodi

Per preparare l'installazione iniziale di StorageGRID, installare prima RHEL versione 9,2 e abilitare SSH. Impostare le interfacce di rete, NTP (Network Time Protocol), DNS e il nome host in base alle Best practice. È necessaria almeno un'interfaccia di rete abilitata sulla rete di rete e un'altra per la rete client. Se si utilizza un'interfaccia con codifica VLAN, configurarla come descritto negli esempi seguenti. In caso contrario, sarà sufficiente una semplice configurazione standard dell'interfaccia di rete.

Se è necessario utilizzare un tag VLAN sull'interfaccia di rete della griglia, la configurazione dovrebbe avere due file nel `/etc/sysconfig/network-scripts/` seguente formato:

```
# cat /etc/sysconfig/network-scripts/ifcfg-enp67s0
# This is the parent physical device
TYPE=Ethernet
BOOTPROTO=none
DEVICE=enp67s0
ONBOOT=yes
# cat /etc/sysconfig/network-scripts/ifcfg-enp67s0.520
# The actual device that will be used by the storage node file
DEVICE=enp67s0.520
BOOTPROTO=none
NAME=enp67s0.520
IPADDR=10.10.200.31
PREFIX=24
VLAN=yes
ONBOOT=yes
```

Questo esempio presuppone che il dispositivo di rete fisico per la rete di rete sia enp67s0. Potrebbe anche essere un dispositivo Unito come bond0. Sia che si utilizzi il bonding o un'interfaccia di rete standard, è necessario utilizzare l'interfaccia con codifica VLAN nel file di configurazione del nodo se la porta di rete non dispone di una VLAN predefinita o se la VLAN predefinita non è associata alla rete di rete. Il contenitore StorageGRID stesso non annulla l'etichetta dei frame Ethernet, quindi deve essere gestito dal sistema operativo padre.

Configurazione dello storage opzionale con iSCSI

Se non si utilizza storage iSCSI, è necessario assicurarsi che host1, Host2 e host3 contengano dispositivi a blocchi di dimensioni sufficienti per soddisfare i relativi requisiti. Consultare la sezione "Dimensioni dei dischi per tipo di container" per i requisiti di storage di host1, Host2 e host3.

Per configurare lo storage con iSCSI, attenersi alla seguente procedura:

Fasi

1. Se si utilizza storage iSCSI esterno, ad esempio il software di gestione dei dati NetApp e-Series o NetApp ONTAP®, installare i seguenti pacchetti:

```
sudo yum install iscsi-initiator-utils
sudo yum install device-mapper-multipath
```

2. Individuare l'ID iniziatore su ciascun host.

```
# cat /etc/iscsi/initiatorname.iscsi
InitiatorName=iqn.2006-04.com.example.node1
```

3. Utilizzando il nome dell'iniziatore del passaggio 2, mappare i LUN del dispositivo di archiviazione (del numero e delle dimensioni indicati nella tabella) a ciascun nodo di archiviazione "Requisiti di storage" .
4. Scopri i LUN appena creati `iscsiadm` ed effettua l'accesso.

```
# iscsiadm -m discovery -t st -p target-ip-address
# iscsiadm -m node -T iqn.2006-04.com.example:3260 -l
Logging in to [iface: default, target: iqn.2006-04.com.example:3260,
portal: 10.64.24.179,3260] (multiple)
Login to [iface: default, target: iqn.2006-04.com.example:3260, portal:
10.64.24.179,3260] successful.
```

Per ulteriori informazioni, consultate il "Creazione di un iniziatore iSCSI" portale clienti Red Hat.

5. Per visualizzare i dispositivi multipath e i WWID LUN associati, eseguire il seguente comando:

```
# multipath -ll
```

Se non si utilizza iSCSI con dispositivi multipercorso, è sufficiente montare il dispositivo con un nome di percorso univoco che mantiene le modifiche e il riavvio del dispositivo allo stesso modo.

```
/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0
```

Se i dispositivi vengono rimossi o aggiunti, la semplice utilizzo dei `/dev/sdx` nomi dei dispositivi potrebbe causare problemi in seguito. se si utilizzano dispositivi multipath, modificare il `/etc/multipath.conf` file per utilizzare gli alias come segue.

Questi dispositivi potrebbero essere o meno presenti su tutti i nodi, a seconda del layout.

```
multipaths {
multipath {
wwid 36d039ea00005f06a000003c45fa8f3dc
alias Docker-Store
}
multipath {
wwid 36d039ea00006891b000004025fa8f597
alias Adm-Audit
}
multipath {
wwid 36d039ea00005f06a000003c65fa8f3f0
alias Adm-MySQL
}
multipath {
wwid 36d039ea00006891b000004015fa8f58c
alias Adm-OS
}
multipath {
wwid 36d039ea00005f06a000003c55fa8f3e4
alias SN-OS
}
multipath {
wwid 36d039ea00006891b000004035fa8f5a2
alias SN-Db00
}
multipath {
wwid 36d039ea00005f06a000003c75fa8f3fc
alias SN-Db01
}
multipath {
    wwid 36d039ea00006891b000004045fa8f5af
alias SN-Db02
}
multipath {
wwid 36d039ea00005f06a000003c85fa8f40a
alias GW-OS
}
}
```

Prima di installare Docker nel sistema operativo host, formattare e montare il LUN o il backup del disco `/var/lib/docker`. Le altre LUN sono definite nel file di configurazione del nodo e utilizzate direttamente dai container StorageGRID. In altre parole, non vengono visualizzati nel sistema operativo host; vengono visualizzati nei contenitori stessi e i file system vengono gestiti dall'installatore.

Se si utilizza un LUN con backup iSCSI, inserire nel file fstab qualcosa di simile alla seguente riga. Come notato, gli altri LUN non devono essere montati nel sistema operativo host ma devono essere visualizzati come

dispositivi a blocchi disponibili.

```
/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0 /var/lib/docker ext4
defaults 0 0
```

Preparazione dell'installazione di Docker

Per prepararsi all'installazione di Docker, attenersi alla seguente procedura:

Fasi

1. Crea un file system sul volume di storage Docker su tutti e tre gli host.

   ```
   # sudo mkfs.ext4 /dev/sd?
   ```

   Se si utilizzano dispositivi iSCSI con multipath, utilizzare `/dev/mapper/Docker-Store`.

2. Creare il punto di montaggio del volume di storage Docker:

   ```
   # sudo mkdir -p /var/lib/docker
   ```

3. Aggiungere una voce simile per la periferica-volume-archiviazione-docker a `/etc/fstab`.

   ```
   /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0 /var/lib/docker ext4
   defaults 0 0
   ```

   L'opzione seguente `_netdev` è consigliata solo se si utilizza un dispositivo iSCSI. Se si utilizza un dispositivo di blocco locale `_netdev` non è necessario ed `defaults` è consigliato.

   ```
   /dev/mapper/Docker-Store /var/lib/docker ext4 _netdev 0 0
   ```

4. Montare il nuovo file system e visualizzare l'utilizzo del disco.

   ```
   # sudo mount /var/lib/docker
   [root@host1]# df -h | grep docker
   /dev/sdb 200G 33M 200G 1% /var/lib/docker
   ```

5. Disattivare lo swap e disattivarlo per motivi di prestazioni.

   ```
   $ sudo swapoff --all
   ```

6. Per mantenere le impostazioni, rimuovete tutte le voci di swap da /etc/fstab come:

```
/dev/mapper/rhel-swap swap defaults 0 0
```

La mancata disattivazione completa dello swap può ridurre notevolmente le performance.

7. Eseguire un riavvio di prova del nodo per verificare che il `/var/lib/docker` volume sia persistente e che tutti i dispositivi disco ritornino.

Installa Docker per StorageGRID

Scopri come installare Docker per StorageGRID.

Per installare Docker, attenersi alla procedura illustrata di seguito:

Fasi

1. Configurazione del repo yum per Docker.

```
sudo yum install -y yum-utils
sudo yum-config-manager --add-repo \
https://download.docker.com/linux/rhel/docker-ce.repo
```

2. Installare i pacchetti necessari.

```
sudo yum install docker-ce docker-ce-cli containerd.io
```

3. Avviate Docker.

```
sudo systemctl start docker
```

4. Testa Docker.

```
sudo docker run hello-world
```

5. Assicurati che Docker venga eseguito all'avvio del sistema.

```
sudo systemctl enable docker
```

Preparare i file di configurazione dei nodi per StorageGRID

Scopri come preparare i file di configurazione dei nodi per StorageGRID.

Ad un livello alto, il processo di configurazione dei nodi include i seguenti passaggi:

Fasi

1. Creare la `/etc/storagegrid/nodes` directory su tutti gli host.

```
sudo [root@host1 ~]# mkdir -p /etc/storagegrid/nodes
```

2. Creare i file necessari per ciascun host fisico in modo che corrispondano al layout del tipo di container/nodo. In questo esempio, sono stati creati due file per host fisico su ciascun computer host.

> Il nome del file definisce il nome del nodo effettivo per l'installazione. Ad esempio, `dc1-adm1.conf` diventa un nodo denominato `dc1-adm1`.

— Host1:
`dc1-adm1.conf`
`dc1-sn1.conf`

— Host2:
`dc1-gw1.conf`
`dc1-sn2.conf`

— Host3:
`dc1-gw2.conf`
`dc1-sn3.conf`

Preparazione dei file di configurazione del nodo

I seguenti esempi utilizzano il `/dev/disk/by-path` formato. È possibile verificare i percorsi corretti eseguendo i seguenti comandi:

```
[root@host1 ~]# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 90G 0 disk
├─sda1 8:1 0 1G 0 part /boot
└─sda2 8:2 0 89G 0 part
├─rhel-root 253:0 0 50G 0 lvm /
├─rhel-swap 253:1 0 9G 0 lvm
└─rhel-home 253:2 0 30G 0 lvm /home
sdb 8:16 0 200G 0 disk /var/lib/docker
sdc 8:32 0 90G 0 disk
sdd 8:48 0 200G 0 disk
sde 8:64 0 200G 0 disk
sdf 8:80 0 4T 0 disk
sdg 8:96 0 4T 0 disk
sdh 8:112 0 4T 0 disk
sdi 8:128 0 90G 0 disk
sr0 11:0 1 1024M 0 rom
```

E questi comandi:

```
[root@host1 ~]# ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:02:01.0-ata-1.0 ->
../../sr0
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:4:0 ->
../../sde
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:5:0 ->
../../sdf
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:6:0 ->
../../sdg
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:8:0 ->
../../sdh
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:9:0 ->
../../sdi
```

Esempio per il nodo Admin primario

Nome file di esempio:

```
/etc/storagegrid/nodes/dc1-adm1.conf
```

Contenuto del file di esempio:

> I percorsi del disco possono seguire gli esempi riportati di seguito o utilizzare la `/dev/mapper/alias` denominazione dello stile. Non utilizzare i nomi dei dispositivi di blocco, ad esempio `/dev/sdb` perché possono cambiare al riavvio e causare gravi danni alla griglia.

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
MAXIMUM_RAM = 24g
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:2:0
BLOCK_DEVICE_AUDIT_LOGS = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:3:0
BLOCK_DEVICE_TABLES = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:4:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.43
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_IP = 10.193.205.43
CLIENT_NETWORK_MASK = 255.255.255.0
CLIENT_NETWORK_GATEWAY = 10.193.205.1
```

Esempio di un nodo storage

Nome file di esempio:

```
/etc/storagegrid/nodes/dc1-sn1.conf
```

Contenuto del file di esempio:

```
NODE_TYPE = VM_Storage_Node
MAXIMUM_RAM = 24g
ADMIN_IP = 10.193.174.43
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:9:0
BLOCK_DEVICE_RANGEDB_00 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:5:0
BLOCK_DEVICE_RANGEDB_01 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:6:0
BLOCK_DEVICE_RANGEDB_02 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:8:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.44
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
```

Esempio per nodo gateway

Nome file di esempio:

```
/etc/storagegrid/nodes/dc1-gw1.conf
```

Contenuto del file di esempio:

```
NODE_TYPE = VM_API_Gateway
MAXIMUM_RAM = 24g
ADMIN_IP = 10.193.204.43
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.47
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
CLIENT_NETWORK_IP = 10.193.205.47
CLIENT_NETWORK_MASK = 255.255.255.0
CLIENT_NETWORK_GATEWAY = 10.193.205.1
```

Installare dipendenze e pacchetti StorageGRID

Scopri come installare le dipendenze e i pacchetti StorageGRID.

Per installare le dipendenze e i pacchetti di StorageGRID, eseguire i seguenti comandi:

```
[root@host1 rpms]# yum install -y python-netaddr
[root@host1 rpms]# rpm -ivh StorageGRID-Webscale-Images-*.rpm
[root@host1 rpms]# rpm -ivh StorageGRID-Webscale-Service-*.rpm
```

Convalidare i file di configurazione di StorageGRID

Scopri come convalidare il contenuto dei file di configurazione per StorageGRID.

Dopo aver creato i file di configurazione in `/etc/storagegrid/nodes` per ciascuno dei nodi StorageGRID, è necessario convalidare il contenuto di tali file.

Per convalidare il contenuto dei file di configurazione, eseguire il seguente comando su ciascun host:

```
sudo storagegrid node validate all
```

Se i file sono corretti, l'output mostra SUPERATO per ogni file di configurazione:

```
Checking for misnamed node configuration files… PASSED
Checking configuration file for node dc1-adm1… PASSED
Checking configuration file for node dc1-gw1… PASSED
Checking configuration file for node dc1-sn1… PASSED
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes… PASSED
```

Se i file di configurazione non sono corretti, i problemi vengono visualizzati come AVVISI ed ERRORI. Se vengono rilevati errori di configurazione, è necessario correggerli prima di procedere con l'installazione.

```
Checking for misnamed node configuration files…
  WARNING: ignoring /etc/storagegrid/nodes/dc1-adm1
  WARNING: ignoring /etc/storagegrid/nodes/dc1-sn2.conf.keep
  WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dc1-adm1…
  ERROR: NODE_TYPE = VM_Foo_Node
         VM_Foo_Node is not a valid node type.  See *.conf.sample
  ERROR: ADMIN_ROLE = Foo
         Foo is not a valid admin role.  See *.conf.sample
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
         /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dc1-gw1…
  ERROR: GRID_NETWORK_TARGET = bond0.1001
         bond0.1001 is not a valid interface.  See `ip link show`
  ERROR: GRID_NETWORK_IP = 10.1.3
         10.1.3 is not a valid IPv4 address
  ERROR: GRID_NETWORK_MASK = 255.248.255.0
         255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dc1-sn1…
  ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
         10.2.0.1 is not on the local subnet
  ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
         Could not parse subnet list
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes…
  ERROR: GRID_NETWORK_IP = 10.1.0.4
         dc1-sn2 and dc1-sn3 have the same GRID_NETWORK_IP
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
  ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_RANGEDB_00
```

Avviare il servizio host StorageGRID

Informazioni su come avviare il servizio host StorageGRID.

Per avviare i nodi StorageGRID e assicurarsi che vengano riavviati dopo il riavvio dell'host, è necessario attivare e avviare il servizio host StorageGRID.

Per avviare il servizio host StorageGRID, attenersi alla procedura riportata di seguito.

Fasi

1. Eseguire i seguenti comandi su ciascun host:

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

   Il processo di avvio potrebbe richiedere del tempo durante l'esecuzione iniziale.

2. Eseguire il seguente comando per assicurarsi che l'implementazione stia procedendo:

```
sudo storagegrid node status node-name
```

3. Per qualsiasi nodo che restituisce uno stato di `Not-Running` o `Stopped`, eseguire il comando seguente:

```
sudo storagegrid node start node-name
```

   Ad esempio, dato il seguente output si avvierebbe il `dc1-adm1` nodo:

```
[user@host1]# sudo storagegrid node status
Name Config-State Run-State
dc1-adm1 Configured Not-Running
dc1-sn1 Configured Running
```

4. Se in precedenza è stato attivato e avviato il servizio host StorageGRID (o se non si è certi che il servizio sia stato attivato e avviato), eseguire anche il seguente comando:

```
sudo systemctl reload-or-restart storagegrid
```

Configurare il gestore di rete in StorageGRID

Informazioni su come configurare il gestore di griglie in StorageGRID sul nodo amministrativo primario.

Completare l'installazione configurando il sistema StorageGRID dall'interfaccia utente di Grid Manager sul

nodo amministrativo primario.

Passaggi di alto livello

La configurazione della griglia e il completamento dell'installazione prevedono le seguenti operazioni:

Fasi

1. Accedere a Grid Manager
2. "Specificare le informazioni sulla licenza StorageGRID"
3. "Aggiungere siti a StorageGRID"
4. "Specificare le subnet della rete griglia"
5. "Approvare i nodi griglia in sospeso"
6. "Specificare le informazioni sul server NTP"
7. "Specificare le informazioni sul server del sistema dei nomi di dominio"
8. "Specificare le password di sistema di StorageGRID"
9. "Esaminare la configurazione e completare l'installazione"

Accedere a Grid Manager

Utilizzare Gestione griglia per definire tutte le informazioni necessarie per configurare il sistema StorageGRID.

Prima di iniziare, il nodo amministrativo primario deve essere distribuito e aver completato la sequenza di avvio iniziale.

Per utilizzare Grid Manager per definire le informazioni, attenersi alla seguente procedura.

Fasi

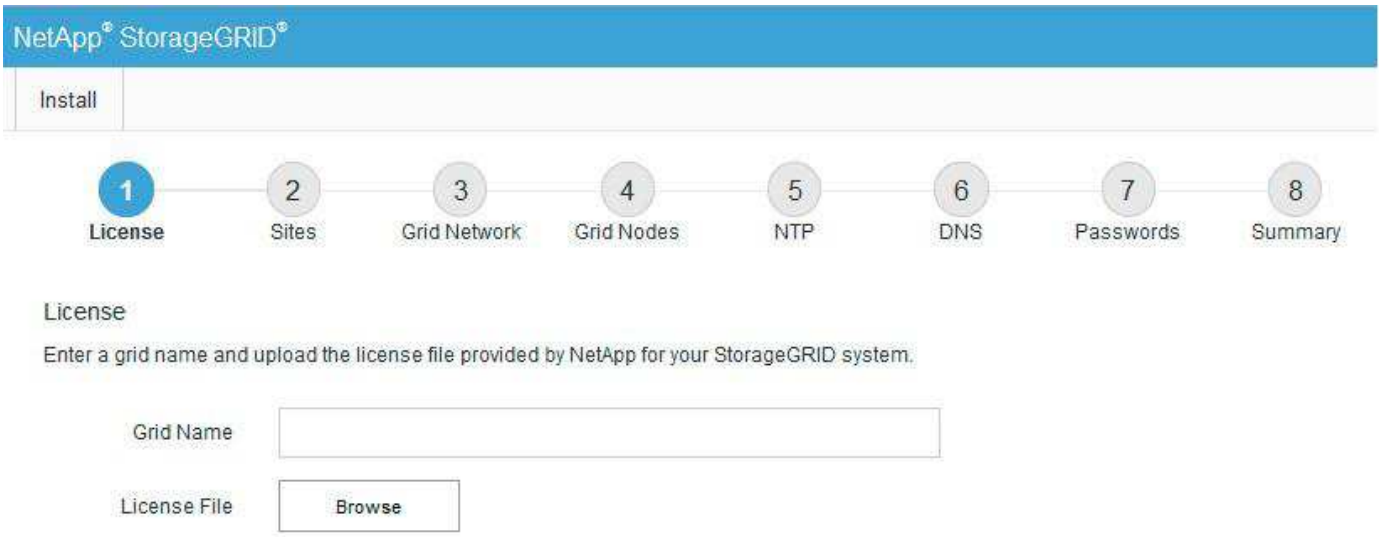
1. Accedere a Grid Manager al seguente indirizzo:

   ```
   https://primary_admin_node_grid_ip
   ```

   In alternativa, è possibile accedere a Grid Manager sulla porta 8443.

   ```
   https://primary_admin_node_ip:8443
   ```

2. Fare clic su Installa un sistema StorageGRID. Viene visualizzata la pagina utilizzata per configurare una griglia StorageGRID.



Aggiungere i dettagli della licenza StorageGRID

Informazioni su come caricare il file di licenza StorageGRID.

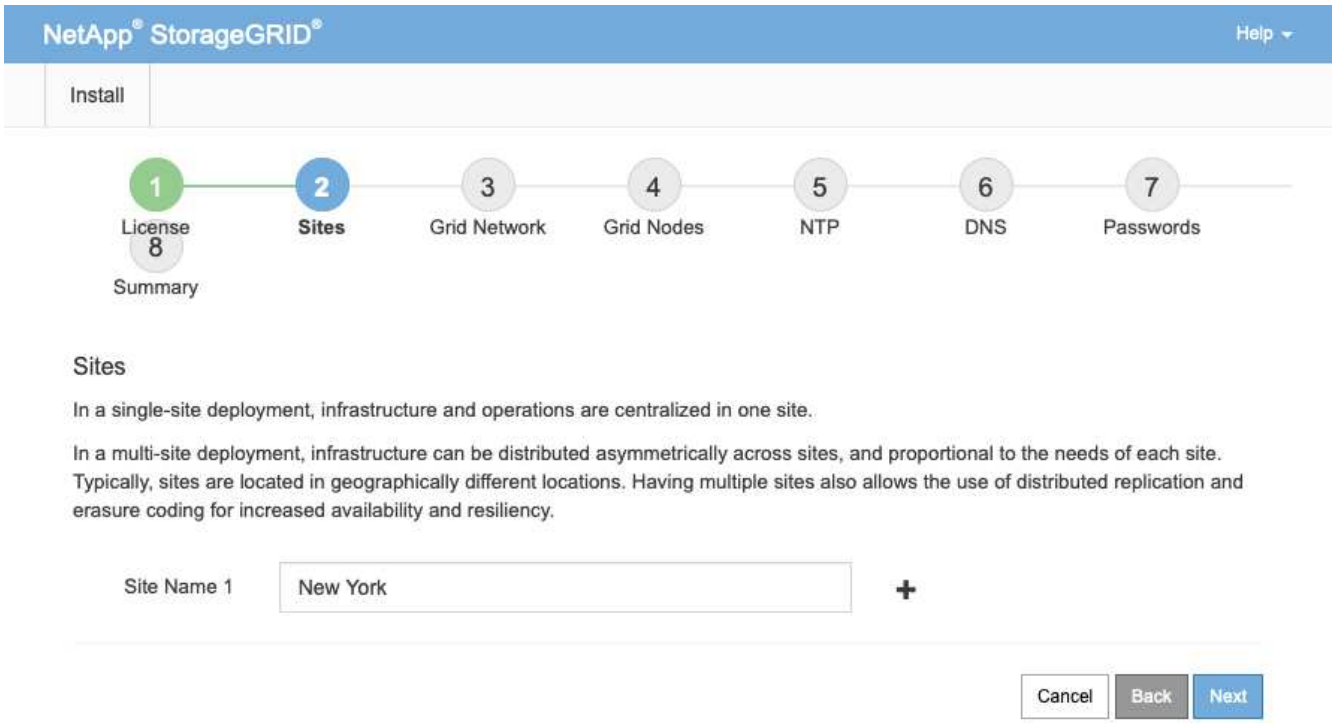
Specificare il nome del sistema StorageGRID e caricare il file di licenza fornito da NetApp.

Per specificare le informazioni sulla licenza StorageGRID, attenersi alla seguente procedura:

Fasi

1. Nella pagina licenza, nel campo Nome griglia, immettere un nome per il sistema StorageGRID. Dopo l'installazione, il nome viene visualizzato come livello superiore nella struttura della topologia della griglia.
2. Fare clic su Sfoglia, individuare il file di licenza NetApp (`NLF-*unique-id*.txt`e fare clic su Apri. Il file di licenza viene validato e vengono visualizzati il numero di serie e la capacità dello storage concesso in licenza.

> L'archivio di installazione di StorageGRID include una licenza gratuita che non fornisce alcun diritto di supporto per il prodotto. È possibile eseguire l'aggiornamento a una licenza che offra supporto dopo l'installazione.



3. Fare clic su Avanti.

Aggiungere siti a StorageGRID

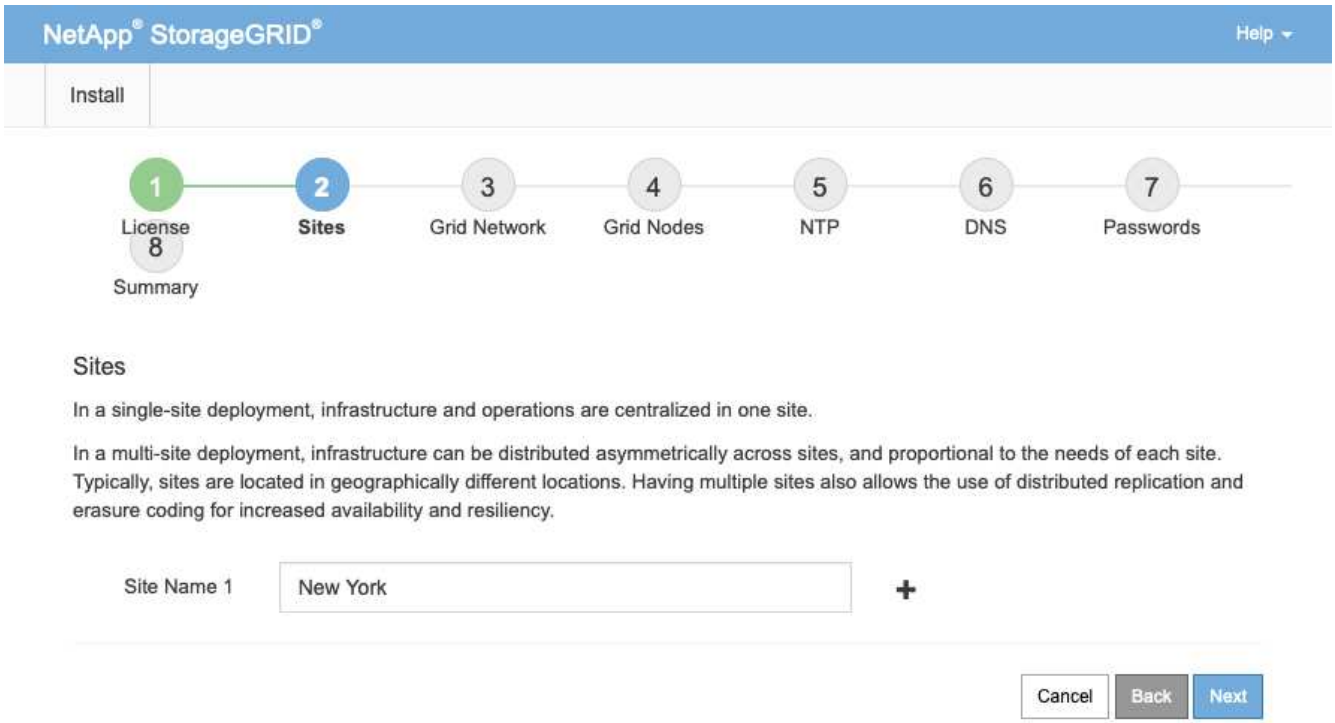
Scopri come aggiungere siti a StorageGRID per aumentare l'affidabilità e la capacità dello storage.

Quando si installa StorageGRID, è necessario creare almeno un sito. È possibile creare siti aggiuntivi per aumentare l'affidabilità e la capacità di storage del sistema StorageGRID.

Per aggiungere siti, attenersi alla seguente procedura:

Fasi

1. Nella pagina Siti, immettere il nome del sito.
2. Per aggiungere altri siti, fare clic sul segno più accanto all'ultima voce del sito e immettere il nome nella nuova casella di testo Nome sito. Aggiungi tutti i siti aggiuntivi necessari per la topologia della griglia. È possibile aggiungere fino a 16 siti.



3. Fare clic su Avanti.

Specificare le subnet di rete della griglia per StorageGRID

Informazioni su come configurare le subnet di rete per StorageGRID.

È necessario specificare le subnet utilizzate sulla rete a griglia.

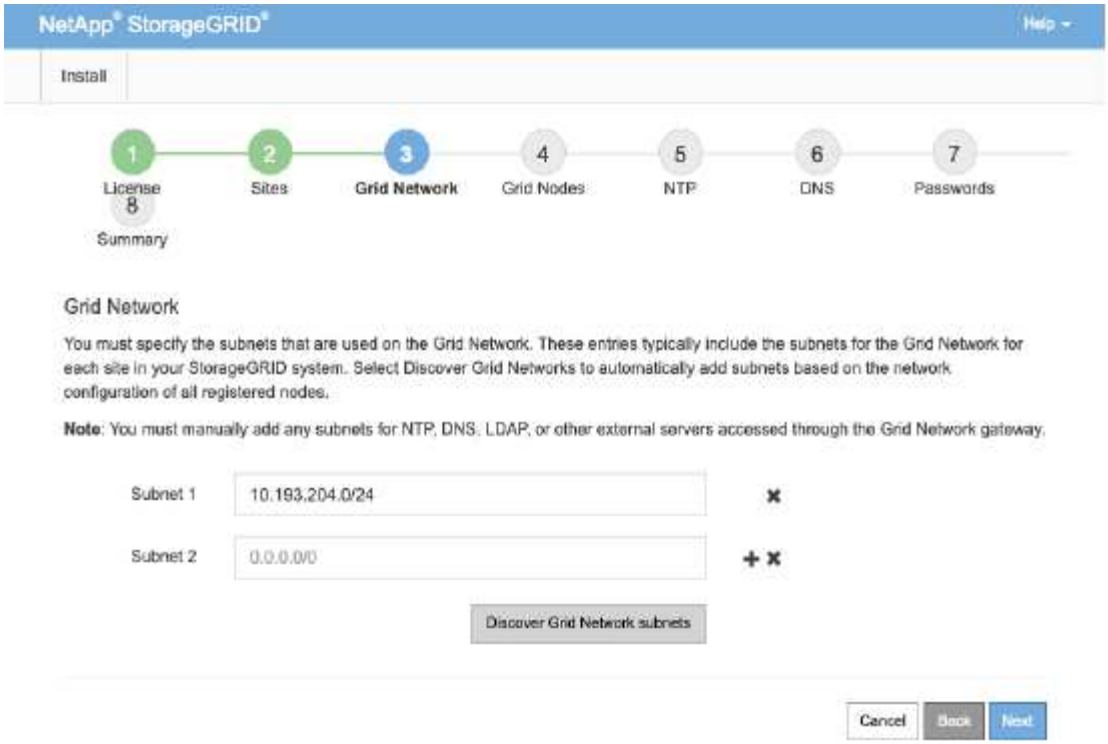
Le voci della subnet includono le subnet per la rete di rete per ogni sito del sistema StorageGRID, oltre alle subnet che devono essere raggiungibili attraverso la rete di rete (ad esempio, le subnet che ospitano i server NTP).

Se si dispone di più sottoreti di rete, è necessario il gateway di rete. Tutte le subnet della griglia specificate devono essere raggiungibili tramite questo gateway.

Per specificare le sottoreti della rete a griglia, attenersi alla seguente procedura:

Fasi

1. Nella casella di testo Subnet 1, specificare l'indirizzo di rete CIDR per almeno una rete a griglia.
2. Fare clic sul segno più accanto all'ultima voce per aggiungere una voce di rete aggiuntiva. Se è già stato distribuito almeno un nodo, fare clic su rileva subnet Grid Networks per compilare automaticamente l'elenco delle subnet della rete griglia con le subnet segnalate dai nodi della griglia registrati con Grid Manager.



3. Fare clic su Avanti.

Approva nodi griglia per StorageGRID

Scopri come esaminare e approvare tutti i nodi grid in sospeso che si uniscono al sistema StorageGRID.

È necessario approvare ciascun nodo griglia prima di unirsi al sistema StorageGRID.

> Prima di iniziare, tutti i nodi grid di appliance virtuali e StorageGRID devono essere implementati.

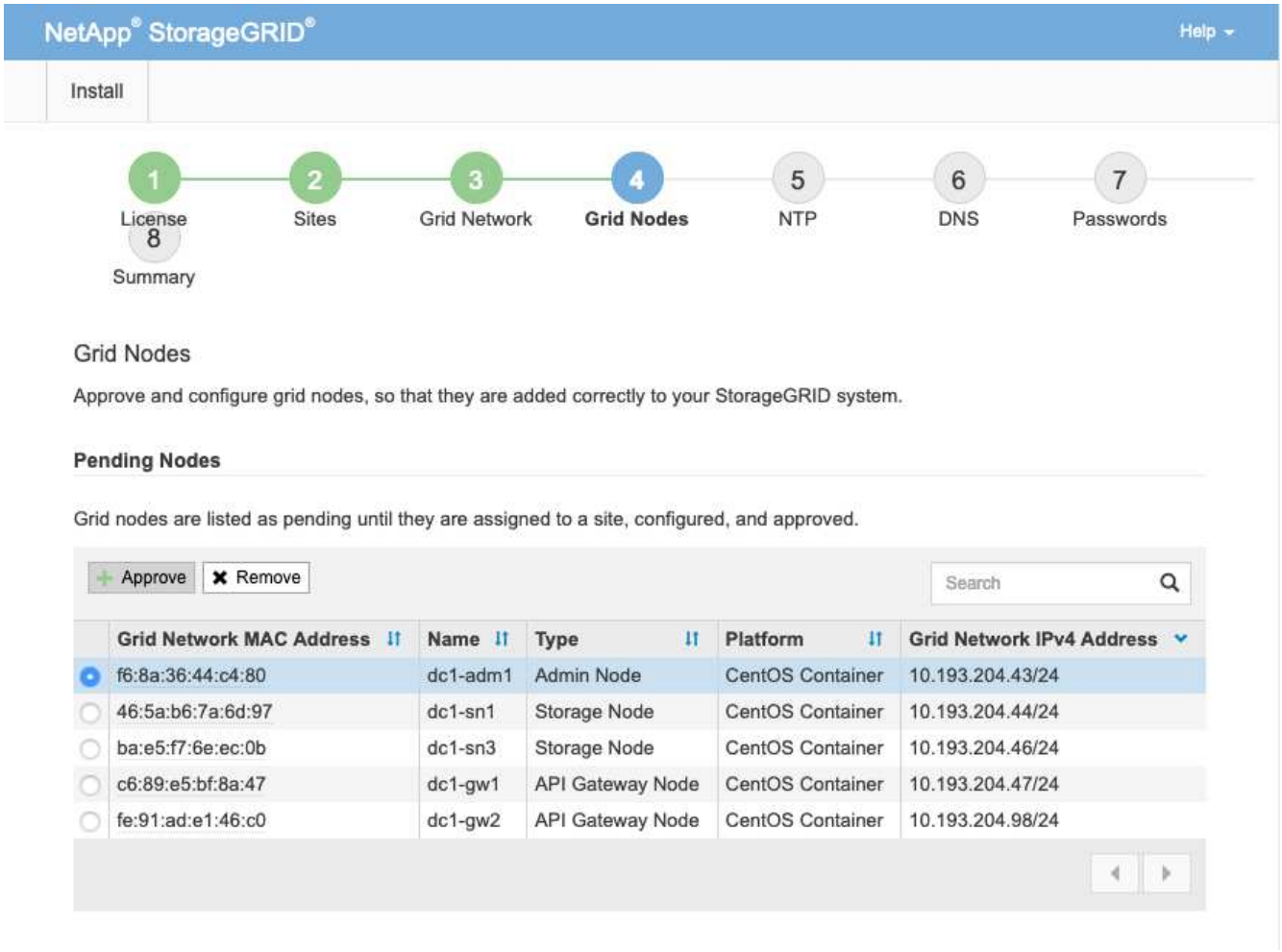
Per approvare i nodi griglia in sospeso, completare i seguenti passaggi:

Fasi

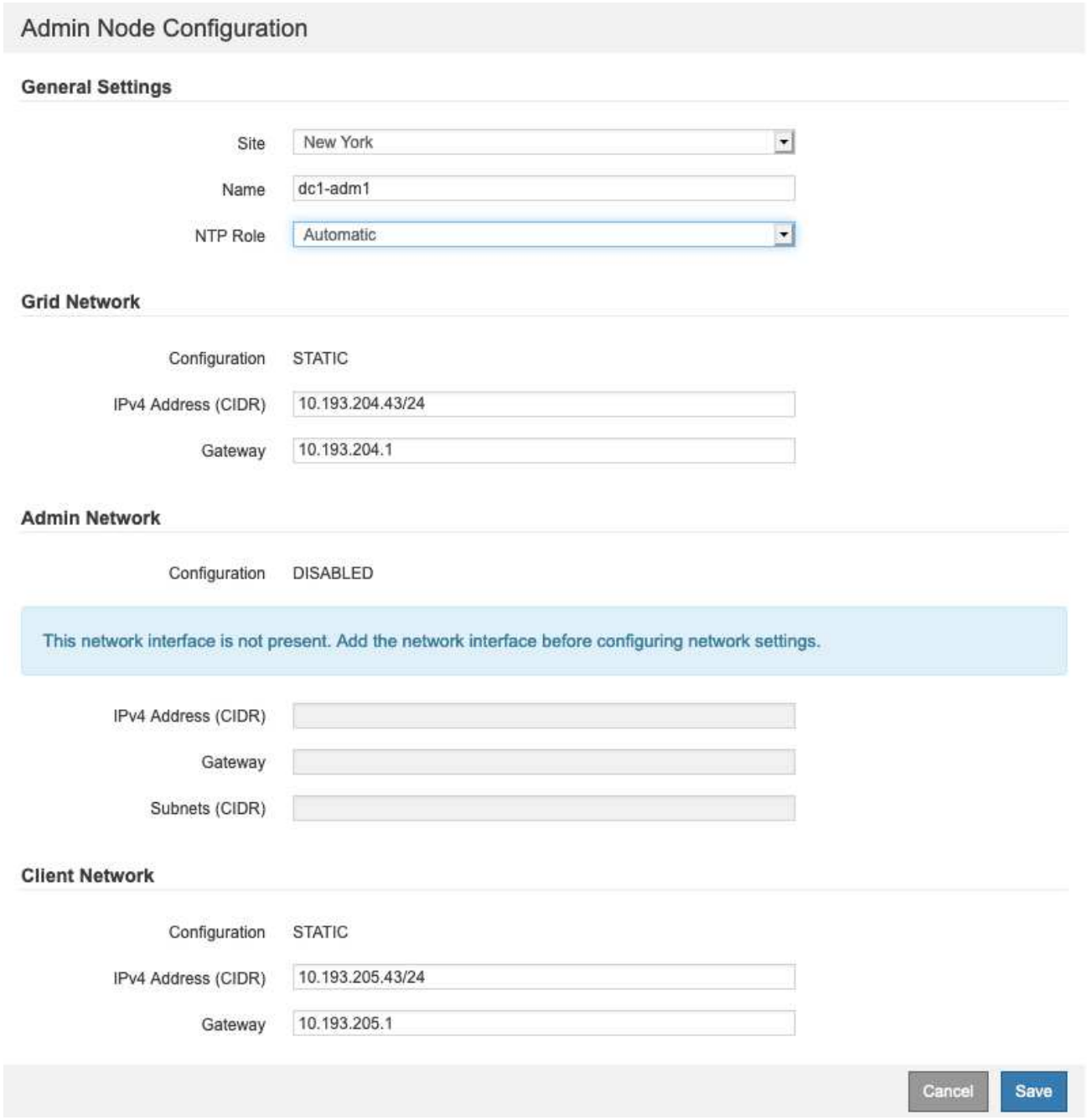
1. Esaminare l'elenco dei nodi in sospeso e verificare che visualizzi tutti i nodi della griglia distribuiti.

   > Se manca un nodo Grid, confermare che è stato implementato correttamente.

2. Fare clic sul pulsante di opzione accanto a un nodo in sospeso che si desidera approvare.



3. Fare clic su approva.
4. In Impostazioni generali, modificare le impostazioni per le seguenti proprietà, se necessario.



— **Sito**: Il nome del sistema del sito per questo nodo della griglia.

— **Nome**: Il nome host che verrà assegnato al nodo e il nome che verrà visualizzato in Grid Manager. Per impostazione predefinita, il nome è quello specificato durante la distribuzione dei nodi, ma è possibile modificarlo in base alle esigenze.

— **ruolo NTP**: Il ruolo NTP del nodo grid. Le opzioni disponibili sono Automatic (automatico), Primary (primario) e Client (Client). Selezionando l'opzione automatico, il ruolo primario viene assegnato ai nodi di amministrazione, ai nodi di archiviazione con i servizi ADC (Administrative Domain Controller), ai nodi gateway e a tutti i nodi di griglia che dispongono di indirizzi IP non statici. A tutti gli altri nodi della griglia viene assegnato il ruolo del client.

Assicurarsi che almeno due nodi di ciascun sito possano accedere ad almeno quattro origini NTP esterne. Se solo un nodo di un sito può raggiungere le origini NTP, si verificheranno problemi di tempistica se tale nodo non funziona. Inoltre, la designazione di due nodi per sito come origini NTP primarie garantisce tempi precisi se un sito viene isolato dal resto della rete.

— **Servizio ADC (solo nodi di archiviazione)**: Selezionare automatico per consentire al sistema di determinare se il nodo richiede il servizio ADC. Il servizio ADC tiene traccia della posizione e della disponibilità dei servizi grid. Almeno tre nodi di archiviazione in ogni sito devono includere il servizio ADC. Non è possibile aggiungere il servizio ADC a un nodo dopo averlo implementato.

5. In rete griglia, modificare le impostazioni per le seguenti proprietà, se necessario:

   — **IPv4 address (CIDR)**: L'indirizzo di rete CIDR per l'interfaccia di rete di rete (eth0 all'interno del contenitore). Ad esempio, `192.168.1.234/24`.

   — **Gateway**: Il gateway di rete. Ad esempio, `192.168.0.1`.

   Se sono presenti più sottoreti di rete, è necessario il gateway.

   Se si seleziona DHCP per la configurazione della rete di rete e si modifica il valore in questo punto, il nuovo valore viene configurato come indirizzo statico sul nodo. Verificare che l'indirizzo IP risultante non sia incluso in un pool di indirizzi DHCP.

6. Per configurare la rete di amministrazione per il nodo della griglia, aggiungere o aggiornare le impostazioni nella sezione Admin Network (rete di amministrazione), se necessario.

   Inserire le subnet di destinazione dei percorsi fuori dall'interfaccia nella casella di testo subnet (CIDR). Se sono presenti più sottoreti amministrative, è necessario il gateway amministratore.

   Se si seleziona DHCP per la configurazione della rete amministrativa e si modifica il valore in questo campo, il nuovo valore viene configurato come indirizzo statico sul nodo. Verificare che l'indirizzo IP risultante non sia incluso in un pool di indirizzi DHCP.

   Dispositivi: Per un dispositivo StorageGRID, se la rete di amministrazione non è stata configurata durante l'installazione iniziale utilizzando il programma di installazione del dispositivo StorageGRID, non è possibile configurarla in questa finestra di dialogo Gestione griglia. È invece necessario attenersi alla seguente procedura:

   a. Riavviare il dispositivo: In Appliance Installer, selezionare **Advanced › Reboot** (Avanzate[Riavvia]). Il riavvio può richiedere alcuni minuti.
   b. Selezionare **Configura rete › Configurazione collegamento** e abilitare le reti appropriate.
   c. Selezionare **Configura rete › Configurazione IP** e configurare le reti abilitate.
   d. Tornare alla Home page e fare clic su Start Installation (Avvia installazione).
   e. In Grid Manager: Se il nodo è elencato nella tabella dei nodi approvati, reimpostare il nodo.
   f. Rimuovere il nodo dalla tabella Pending Nodes (nodi in sospeso).
   g. Attendere che il nodo riappaia nell'elenco Pending Nodes (nodi in sospeso).
   h. Confermare che è possibile configurare le reti appropriate. Devono essere già popolate con le informazioni fornite nella pagina di configurazione IP. Per ulteriori informazioni, consultare le istruzioni

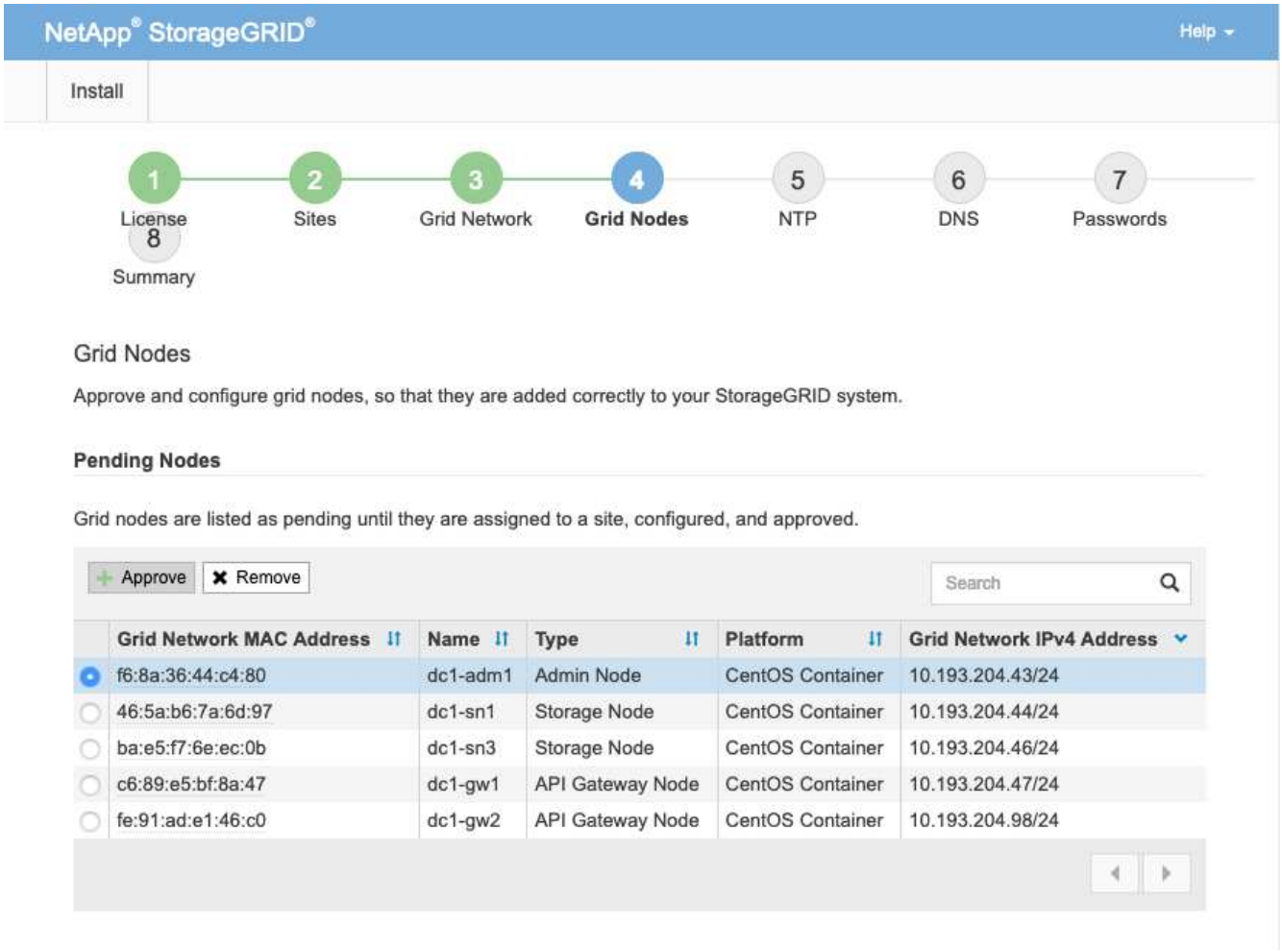
di installazione e manutenzione relative al modello di appliance in uso.

7. Se si desidera configurare la rete client per il nodo Grid, aggiungere o aggiornare le impostazioni nella sezione rete client secondo necessità. Se la rete client è configurata, il gateway è necessario e diventa il gateway predefinito per il nodo dopo l'installazione.

   Dispositivi: Per un dispositivo StorageGRID, se la rete client non è stata configurata durante l'installazione iniziale utilizzando il programma di installazione del dispositivo StorageGRID, non è possibile configurarla in questa finestra di dialogo Gestore griglia. È invece necessario attenersi alla seguente procedura:

   a. Riavviare il dispositivo: In Appliance Installer, selezionare **Advanced › Reboot** (Avanzate[Riavvia]). Il riavvio può richiedere alcuni minuti.
   b. Selezionare **Configura rete › Configurazione collegamento** e abilitare le reti appropriate.
   c. Selezionare **Configura rete › Configurazione IP** e configurare le reti abilitate.
   d. Tornare alla Home page e fare clic su Start Installation (Avvia installazione).
   e. In Grid Manager: Se il nodo è elencato nella tabella dei nodi approvati, reimpostare il nodo.
   f. Rimuovere il nodo dalla tabella Pending Nodes (nodi in sospeso).
   g. Attendere che il nodo riappaia nell'elenco Pending Nodes (nodi in sospeso).
   h. Confermare che è possibile configurare le reti appropriate. Devono essere già popolate con le informazioni fornite nella pagina di configurazione IP. Per ulteriori informazioni, consultare le istruzioni di installazione e manutenzione dell'apparecchio.

8. Fare clic su Salva. La voce del nodo della griglia viene spostata nell'elenco dei nodi approvati.



9. Ripetere i passaggi 1-8 per ogni nodo griglia in sospeso che si desidera approvare.

   È necessario approvare tutti i nodi desiderati nella griglia. Tuttavia, è possibile tornare a questa pagina in qualsiasi momento prima di fare clic su Installa nella pagina Riepilogo. Per modificare le proprietà di un nodo griglia approvato, fare clic sul relativo pulsante di opzione, quindi fare clic su Modifica.

10. Dopo aver approvato i nodi della griglia, fare clic su Avanti.

Specificare i dettagli del server NTP per StorageGRID

Informazioni su come specificare le informazioni di configurazione NTP per il sistema StorageGRID in modo che le operazioni eseguite su server separati possano essere mantenute sincronizzate.

Per evitare problemi di deriva temporale, è necessario specificare quattro riferimenti server NTP esterni dello strato 3 o superiore.

> Quando si specifica l'origine NTP esterna per un'installazione StorageGRID a livello di produzione, non utilizzare il servizio Windows Time (W32Time) su una versione di Windows precedente a Windows Server 2016. Il servizio Time nelle versioni precedenti di Windows non è sufficientemente accurato e non è supportato da Microsoft per l'uso in ambienti complessi come StorageGRID.

I server NTP esterni vengono utilizzati dai nodi ai quali sono stati precedentemente assegnati i ruoli NTP

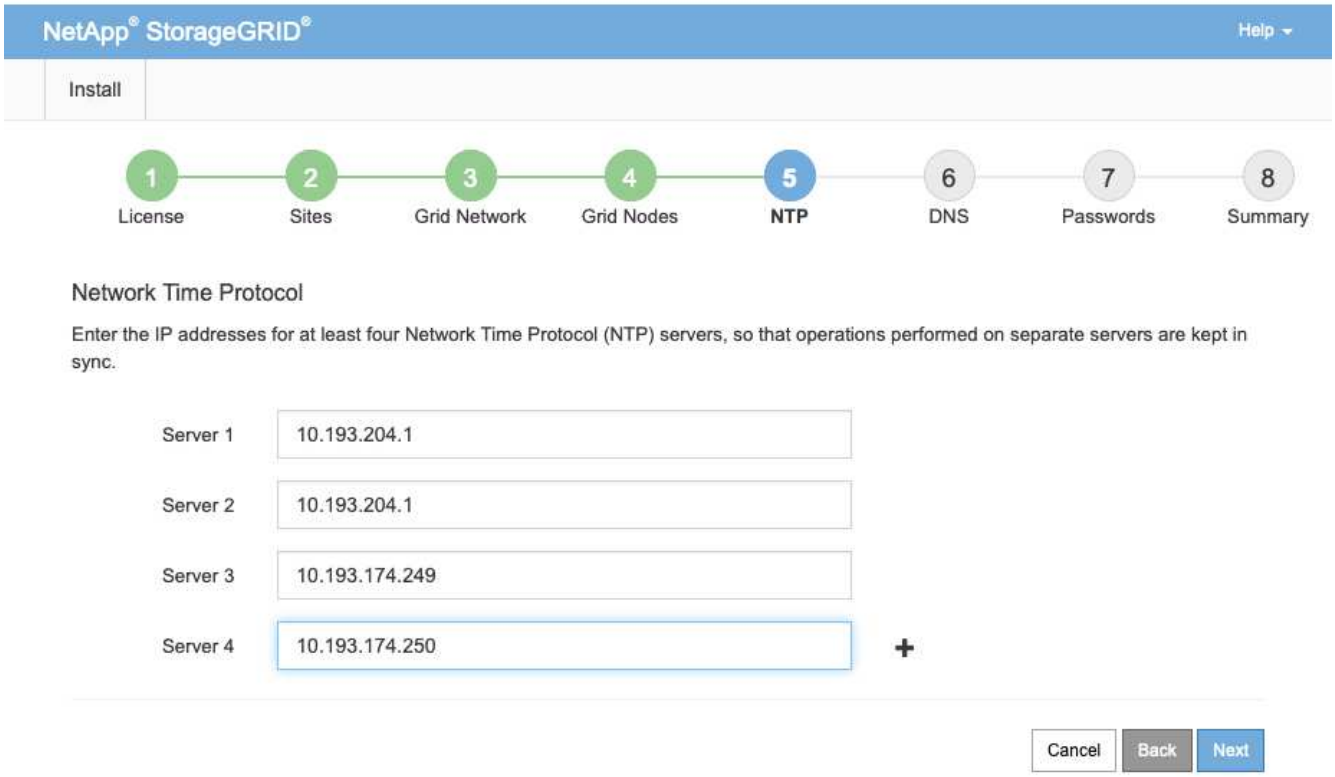
primari.

> La rete client non è abilitata abbastanza presto nel processo di installazione per essere l'unica fonte di server NTP. Assicurarsi che almeno un server NTP possa essere raggiunto sulla rete di rete o sulla rete amministrativa.

Per specificare le informazioni sul server NTP, attenersi alla seguente procedura:

Fasi

1. Nelle caselle di testo Server 1 to Server 4 (Server 1 - Server 2), specificare gli indirizzi IP per almeno quattro server NTP.
2. Se necessario, fare clic sul segno più accanto all'ultima voce per aggiungere altre voci al server.



3. Fare clic su Avanti.

Specificare i dettagli del server DNS per StorageGRID

Informazioni su come configurare il server DNS per StorageGRID.

È necessario specificare le informazioni DNS per il sistema StorageGRID in modo da poter accedere ai server esterni utilizzando nomi host invece di indirizzi IP.

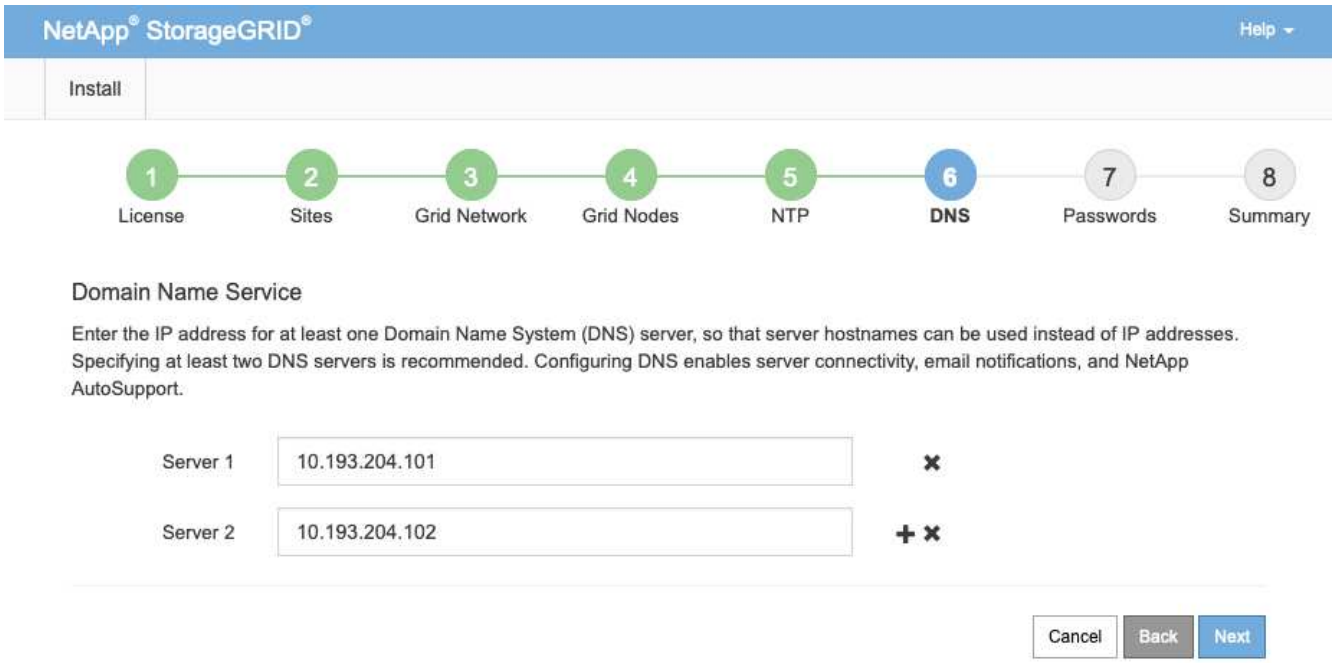
La specifica delle informazioni sul server DNS consente di utilizzare nomi host FQDN (Fully Qualified Domain Name) anziché indirizzi IP per le notifiche e-mail e i messaggi NetApp AutoSupport®. NetApp consiglia di specificare almeno due server DNS.

> Selezionare i server DNS ai quali ciascun sito può accedere localmente in caso di rete.

Per specificare le informazioni sul server DNS, attenersi alla procedura illustrata di seguito:

Fasi

1. Nella casella di testo Server 1, specificare l'indirizzo IP di un server DNS.
2. Se necessario, fare clic sul segno più accanto all'ultima voce per aggiungere altri server.



3. Fare clic su Avanti.

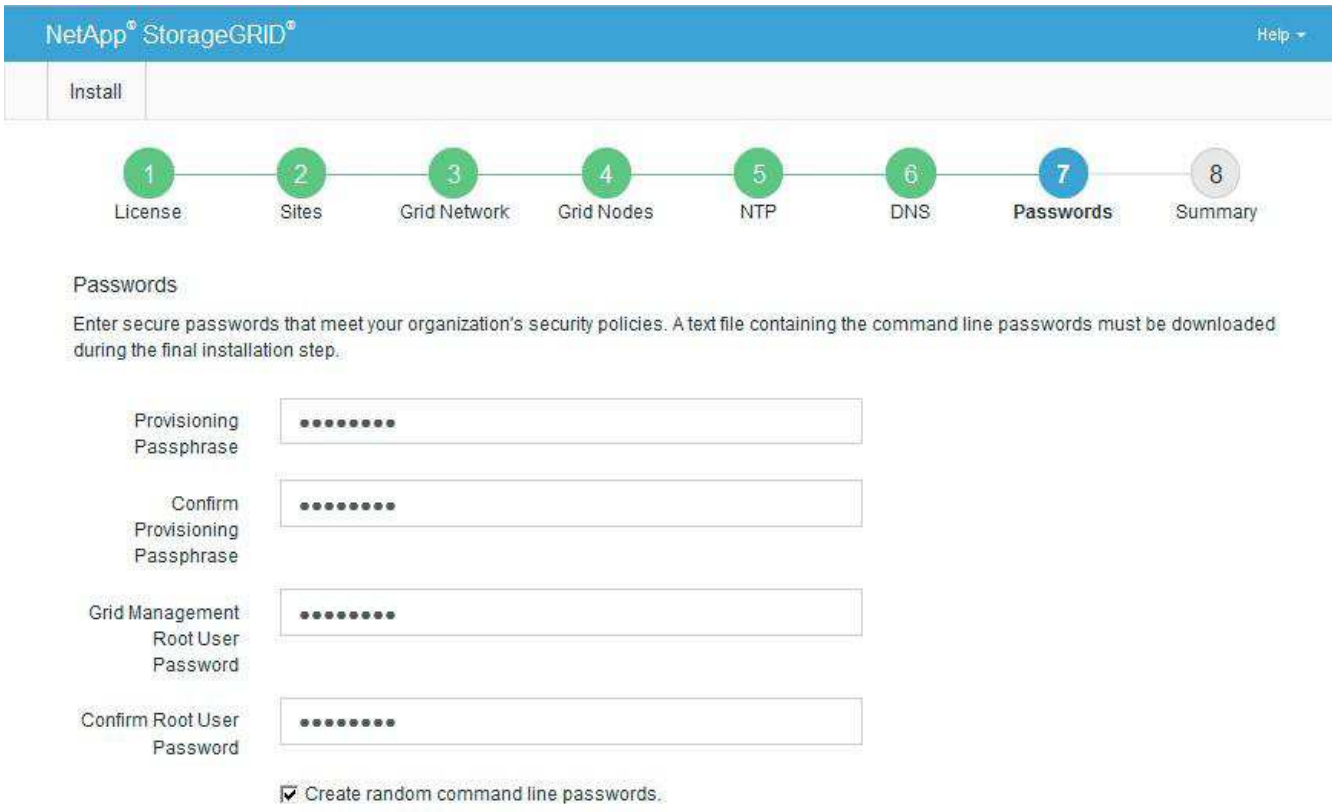
Specificare le password di sistema per StorageGRID

Scoprite come proteggere il vostro sistema StorageGRID impostando la passphrase di provisioning e la password utente root di gestione delle griglie.

Per immettere le password da utilizzare per proteggere il sistema StorageGRID, attenersi alla seguente procedura:

Fasi

1. In Provisioning Passphrase, immettere la passphrase di provisioning necessaria per apportare modifiche alla topologia della griglia del sistema StorageGRID. Registrare la password in un luogo sicuro.
2. In Confirm Provisioning Passphrase (Conferma passphrase di provisioning), immettere nuovamente la passphrase di provisioning.
3. In Grid Management Root User Password (Password utente principale di Grid Management), immettere la password da utilizzare per accedere a Grid Manager come utente root.
4. In Confirm Root User Password (Conferma password utente root), immettere nuovamente la password di Grid Manager.



5. Se si sta installando una griglia per scopi dimostrativi o dimostrativi, deselezionare l'opzione Crea password della riga di comando casuale.

   Per le implementazioni in produzione, le password casuali devono essere sempre utilizzate per motivi di sicurezza. Deselezionare l'opzione Create Random Command Line Passwords (Crea password casuali della riga di comando) solo per le griglie demo se si desidera utilizzare password predefinite per accedere ai nodi della griglia dalla riga di comando utilizzando l'account root o admin.

   > Quando si fa clic su Installa nella pagina Riepilogo, viene richiesto di scaricare il file del pacchetto di ripristino (`sgws-recovery-packageid-revision.zip`. È necessario scaricare questo file per completare l'installazione. Le password di accesso al sistema vengono memorizzate nel `Passwords.txt` file contenuto nel pacchetto di ripristino.

6. Fare clic su Avanti.

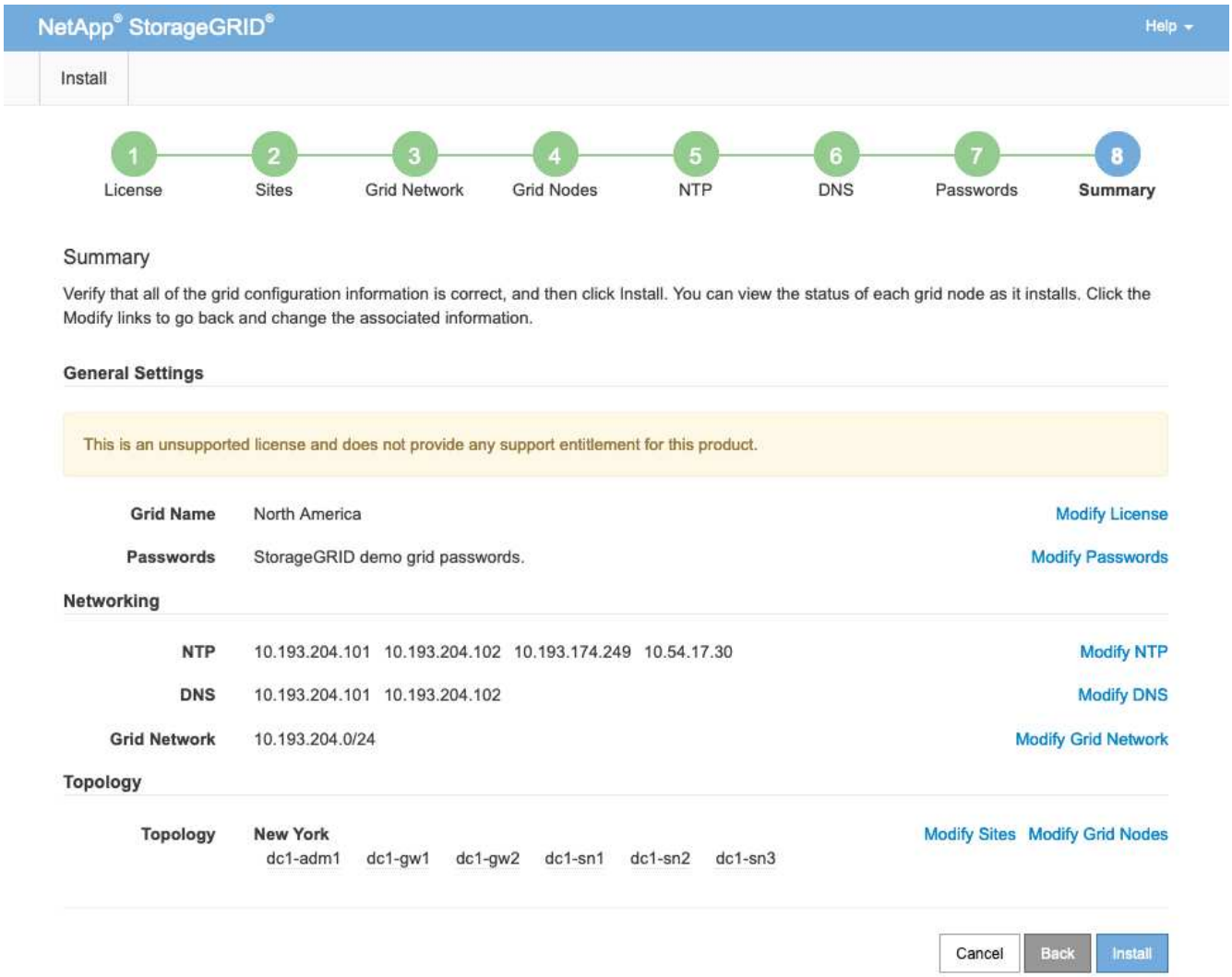
Rivedere la configurazione e completare l'installazione di StorageGRID

Scopri come convalidare le informazioni di configurazione della griglia e completare il processo di installazione di StorageGRID.

Per assicurarsi che l'installazione venga completata correttamente, esaminare attentamente le informazioni di configurazione immesse. Seguire questa procedura.

Fasi

1. Visualizzare la pagina Riepilogo.



2. Verificare che tutte le informazioni di configurazione della griglia siano corrette. Utilizzare i link Modify (Modifica) nella pagina Summary (Riepilogo) per tornare indietro e correggere eventuali errori.
3. Fare clic su Installa.

> Se un nodo è configurato per l'utilizzo della rete client, il gateway predefinito per quel nodo passa dalla rete griglia alla rete client quando si fa clic su Installa. Se si perde la connettività, assicurarsi di accedere al nodo amministrativo primario tramite una subnet accessibile. Per ulteriori informazioni, vedere "Installazione e provisioning della rete".

4. Fare clic su Scarica pacchetto di ripristino.

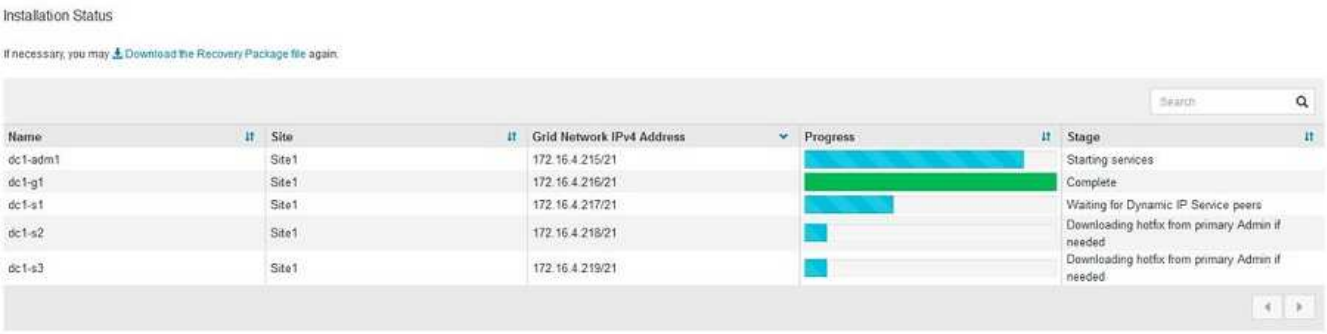
   Quando l'installazione procede fino al punto in cui è definita la topologia della griglia, viene richiesto di scaricare il file del pacchetto di ripristino (`.zip`) e di confermare che è possibile accedere al contenuto di questo file. È necessario scaricare il file del pacchetto di ripristino in modo da poter ripristinare il sistema StorageGRID in caso di errore di uno o più nodi della griglia.

   Verificare che sia possibile estrarre il contenuto del `.zip` file e salvarlo in due posizioni sicure, sicure e separate.

> Il file del pacchetto di ripristino deve essere protetto perché contiene chiavi di crittografia e password che possono essere utilizzate per ottenere dati dal sistema StorageGRID.

5. Selezionare l'opzione ho scaricato e verificato il file del pacchetto di ripristino, quindi fare clic su Avanti.

Se l'installazione è ancora in corso, viene visualizzata la pagina Stato installazione. Questa pagina indica lo stato di avanzamento dell'installazione per ciascun nodo della griglia.



Quando viene raggiunta la fase completa per tutti i nodi della griglia, si apre la pagina di accesso per Grid Manager.

6. Accedere a Grid Manager come utente root con la password specificata durante l'installazione.

Aggiorna i nodi bare-metal in StorageGRID

Scopri il processo di upgrade per i nodi bare-metal in StorageGRID.

Il processo di upgrade per i nodi bare-metal è diverso rispetto ad appliance o nodi VMware. Prima di eseguire un aggiornamento di un nodo bare-metal, è necessario aggiornare i file RPM su tutti gli host prima di eseguire l'aggiornamento tramite la GUI.

```
[root@host1 rpms]# rpm -Uvh StorageGRID-Webscale-Images-*.rpm
[root@host1 rpms]# rpm -Uvh StorageGRID-Webscale-Service-*.rpm
```

A questo punto è possibile procedere all'aggiornamento del software tramite la GUI.

TR-4907: Configurare StorageGRID con veritas Enterprise Vault

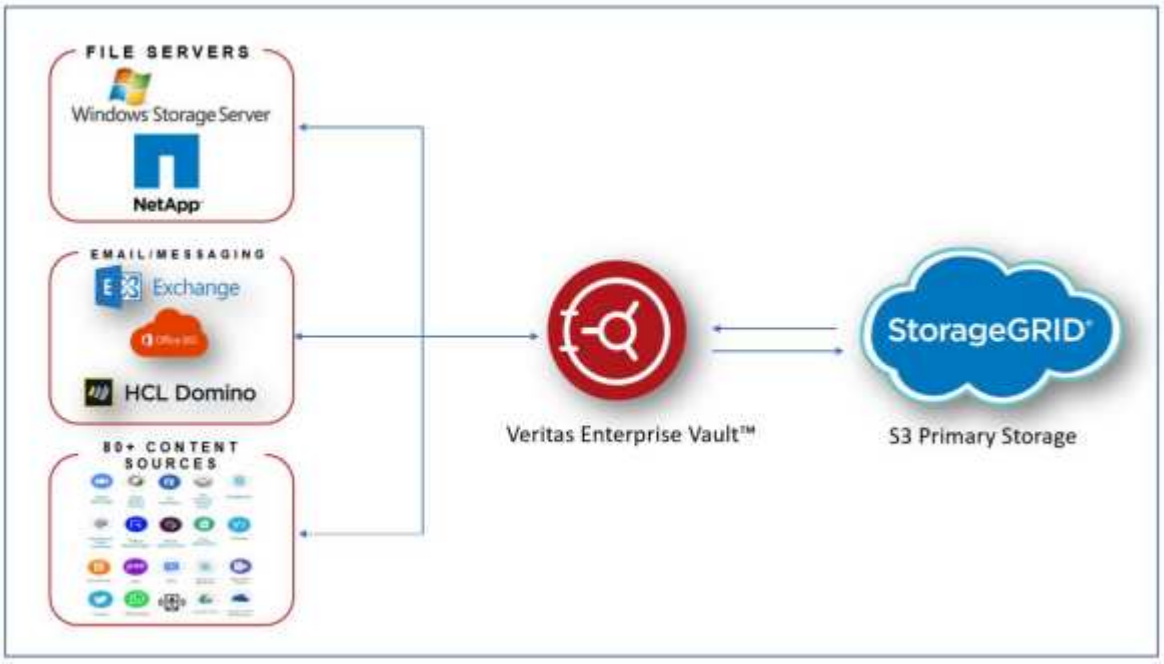
Introduzione alla configurazione di StorageGRID per il failover del sito

Scopri come veritas Enterprise Vault utilizza StorageGRID come destinazione di storage primario per il disaster recovery.

Questa guida alla configurazione fornisce i passaggi per configurare NetApp® StorageGRID® come destinazione di storage primario con veritas Enterprise Vault. Viene inoltre descritto come configurare StorageGRID per il failover del sito in uno scenario di disaster recovery (DR).

Architettura di riferimento

StorageGRID offre una destinazione di backup cloud on-premise compatibile con S3 per veritas Enterprise Vault. La figura seguente illustra l'architettura di veritas Enterprise Vault e StorageGRID.



Dove trovare ulteriori informazioni

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

- Centro di documentazione NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-118/
- Abilitazione NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Documentazione dei prodotti NetApp https://www.netapp.com/support-and-training/documentation/

Configurare StorageGRID e veritas Enterprise Vault

Scopri come implementare le configurazioni di base per StorageGRID 11,5 o versioni successive e veritas Enterprise Vault 14,1 o versioni successive.

Questa guida alla configurazione si basa su StorageGRID 11,5 e Enterprise Vault 14,1. Per lo storage in modalità write once, Read many (WORM) utilizzando blocco degli oggetti S3, StorageGRID 11,6 ed Enterprise Vault 14.2.2. Per informazioni più dettagliate su queste linee guida, visitare la "Documentazione StorageGRID" pagina o contattare un esperto StorageGRID.

Prerequisiti per configurare StorageGRID e veritas Enterprise Vault

- Prima di configurare StorageGRID con veritas Enterprise Vault, verificare i seguenti prerequisiti:

> Per lo storage WORM (blocco oggetti) è richiesto StorageGRID 11,6 o superiore.

- È installato veritas Enterprise Vault 14,1 o versione successiva.

> Per lo storage WORM (blocco degli oggetti), è richiesto Enterprise Vault versione 14.2.2 o superiore.

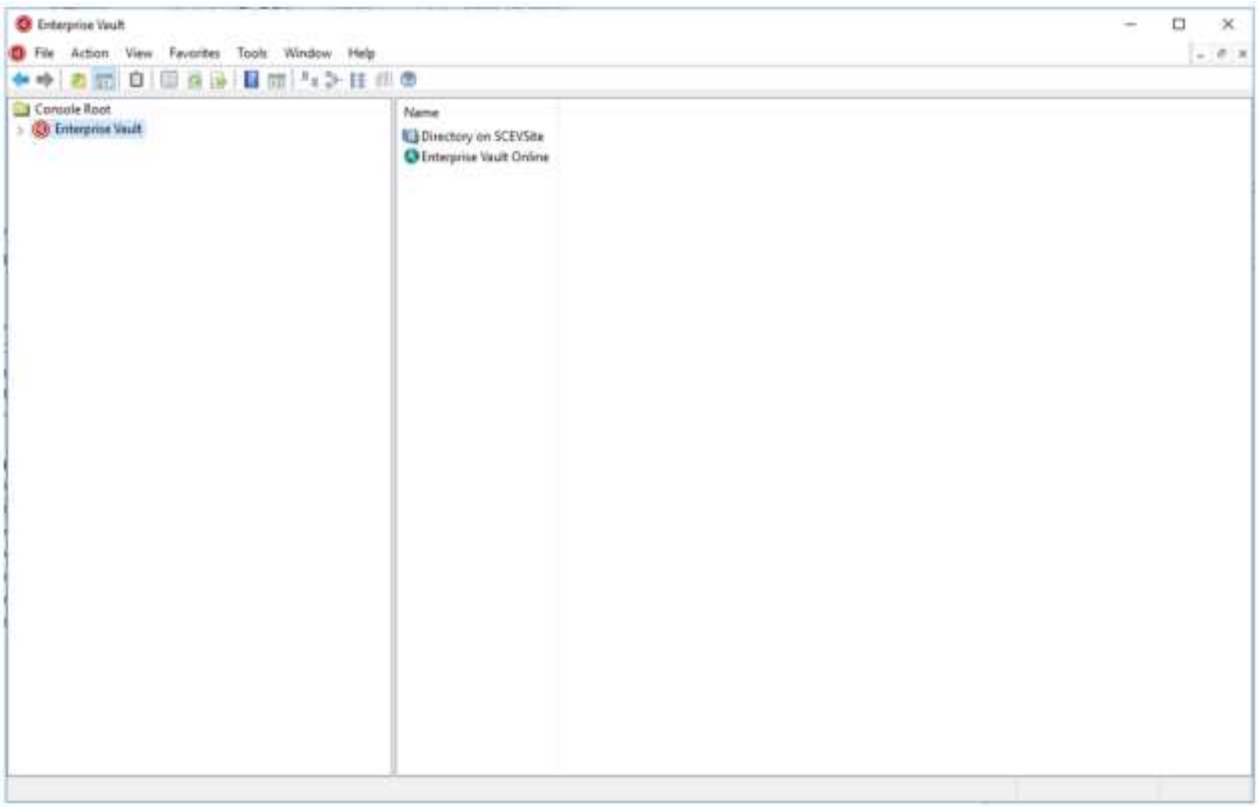
- Sono stati creati gruppi di archivi del vault e un archivio del vault. Per ulteriori informazioni, vedere veritas Enterprise Vault Administration Guide.
- Sono stati creati tenant StorageGRID, chiave di accesso, chiave segreta e bucket.
- È stato creato un endpoint di bilanciamento del carico StorageGRID (HTTP o HTTPS).
- Se si utilizza un certificato autofirmato, aggiungere il certificato CA autofirmato StorageGRID ai server di Enterprise Vault. Per ulteriori informazioni, vedere questo "Articolo della veritas Knowledge base".
- Aggiornare e applicare il file di configurazione del vault Enterprise più recente per abilitare le soluzioni di storage supportate, come NetApp StorageGRID. Per ulteriori informazioni, vedere questo "Articolo della veritas Knowledge base".

Configurare StorageGRID con veritas Enterprise Vault

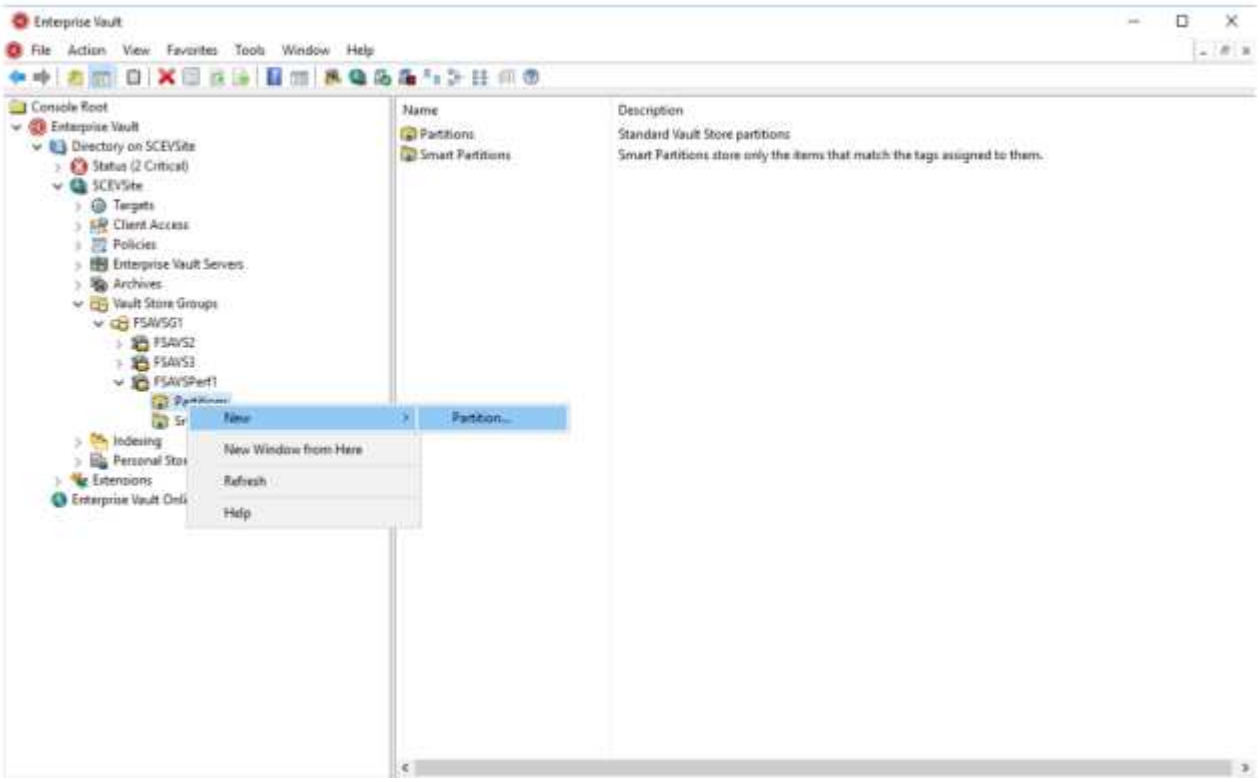
Per configurare StorageGRID con veritas Enterprise Vault, attenersi alla seguente procedura:

Fasi

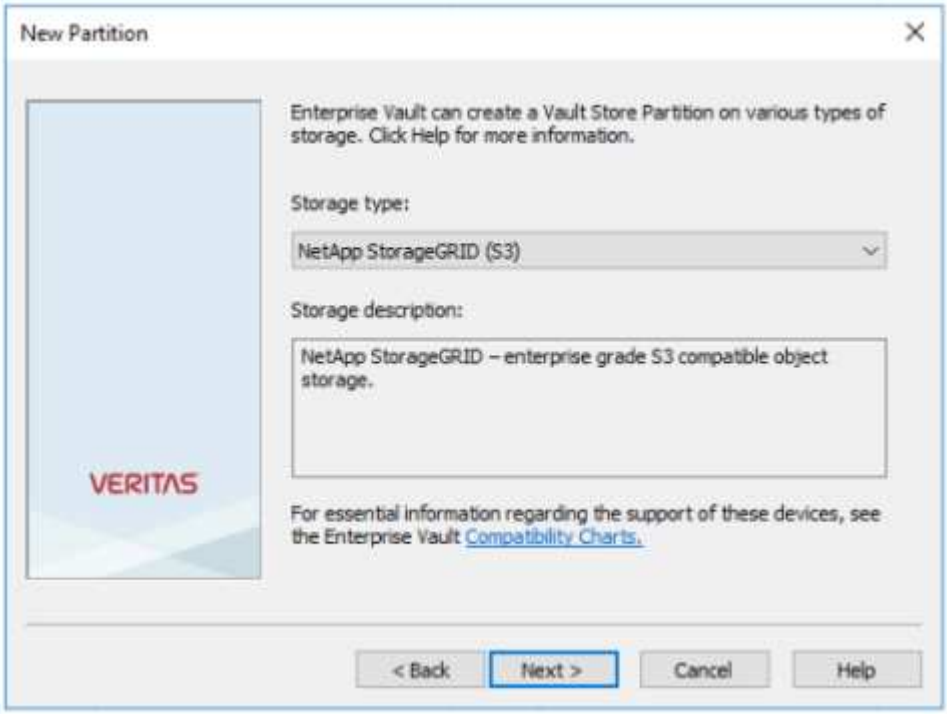
1. Avviare la console di amministrazione di Enterprise Vault.



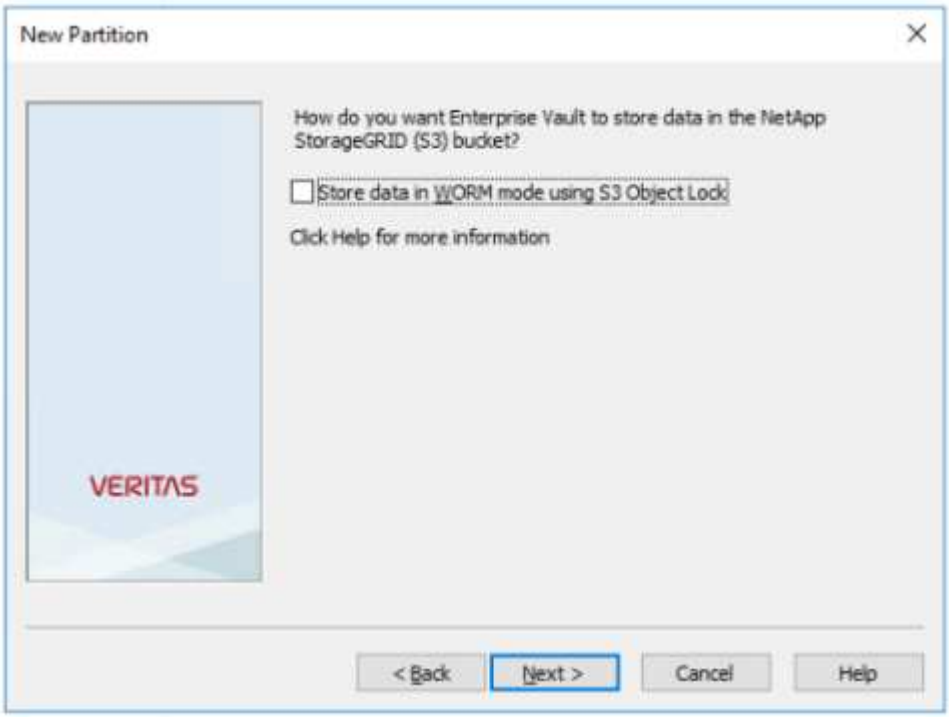
2. Creare una nuova partizione dell'archivio dei vault nell'archivio appropriato. Espandere la cartella Vault Store Groups e quindi l'archivio del vault appropriato. Fare clic con il pulsante destro del mouse su partizione e selezionare **Nuova › partizione**.



3. Seguire la procedura guidata creazione nuova partizione. Dal menu a discesa tipo di archiviazione, selezionare NetApp StorageGRID (S3). Fare clic su Avanti.

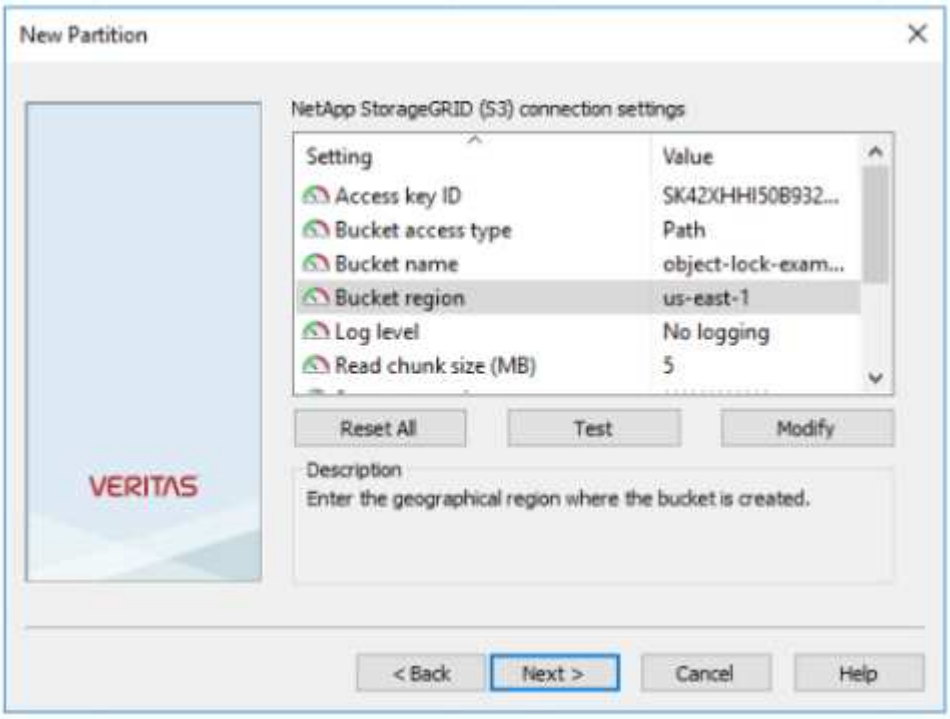


4. Lasciare deselezionata l'opzione Memorizza dati in modalità WORM utilizzando blocco oggetti S3. Fare clic su Avanti.

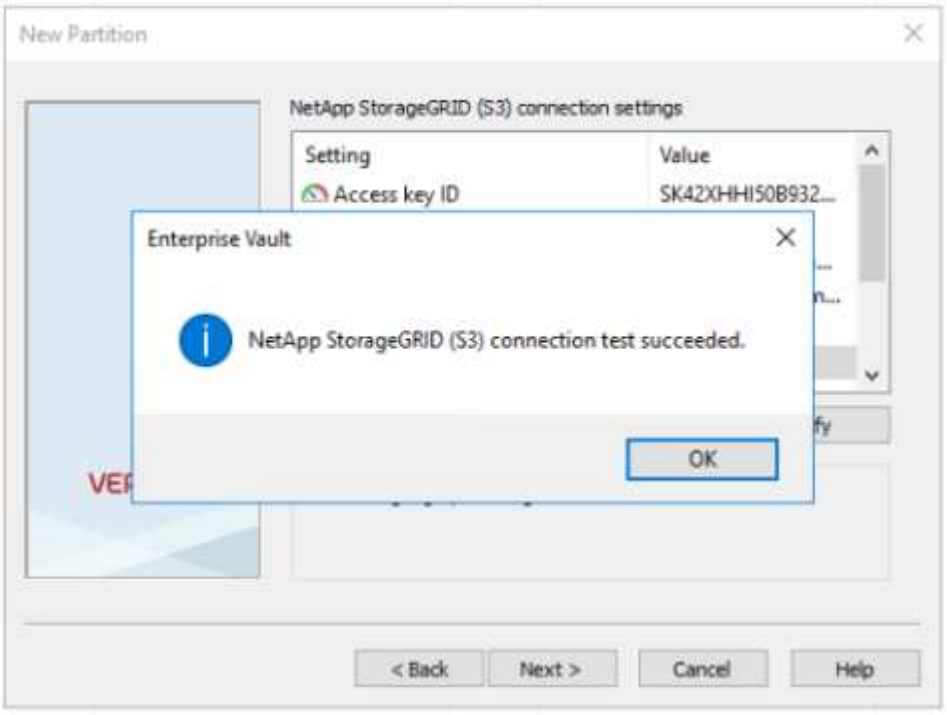


5. Nella pagina delle impostazioni di connessione, fornire le seguenti informazioni:
   - ID chiave di accesso
   - Chiave di accesso segreta
   - Nome host del servizio: Assicurarsi di includere la porta LBE (Load Balancer Endpoint) configurata in StorageGRID (ad esempio https://<hostname>:<LBE_port>)

- Nome bucket: Nome del bucket di destinazione creato in precedenza. veritas Enterprise Vault non crea il bucket.
- Area bucket: `us-east-1` È il valore predefinito.

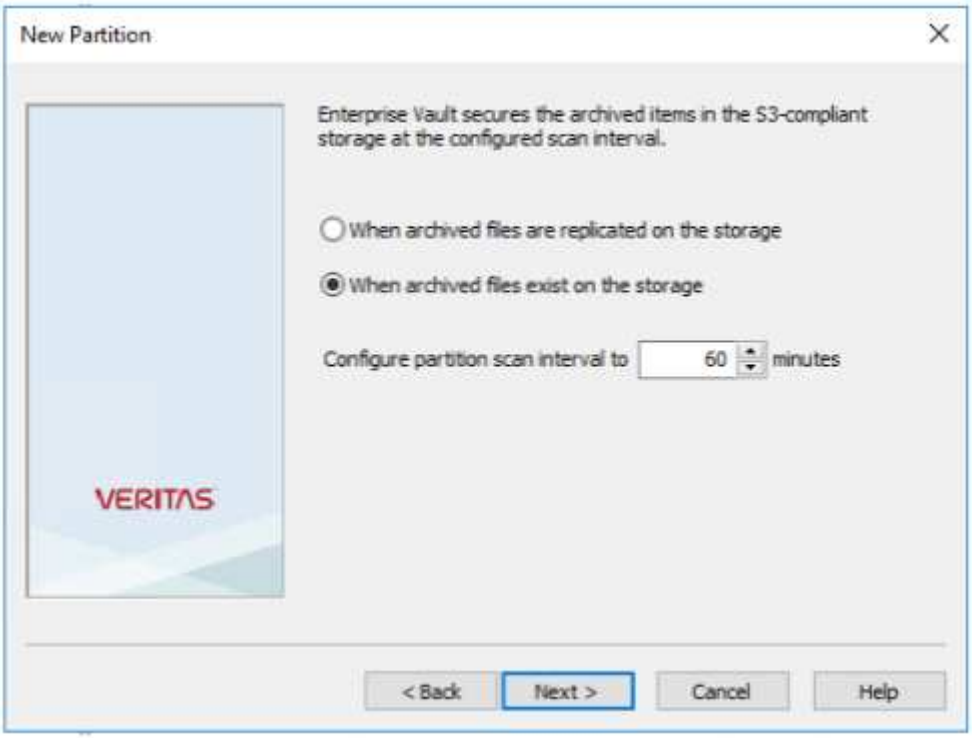


6. Per verificare il collegamento al bucket StorageGRID, fare clic su Test. Verificare che il test di connessione sia stato eseguito correttamente. Fare clic su OK, quindi su Next (Avanti).

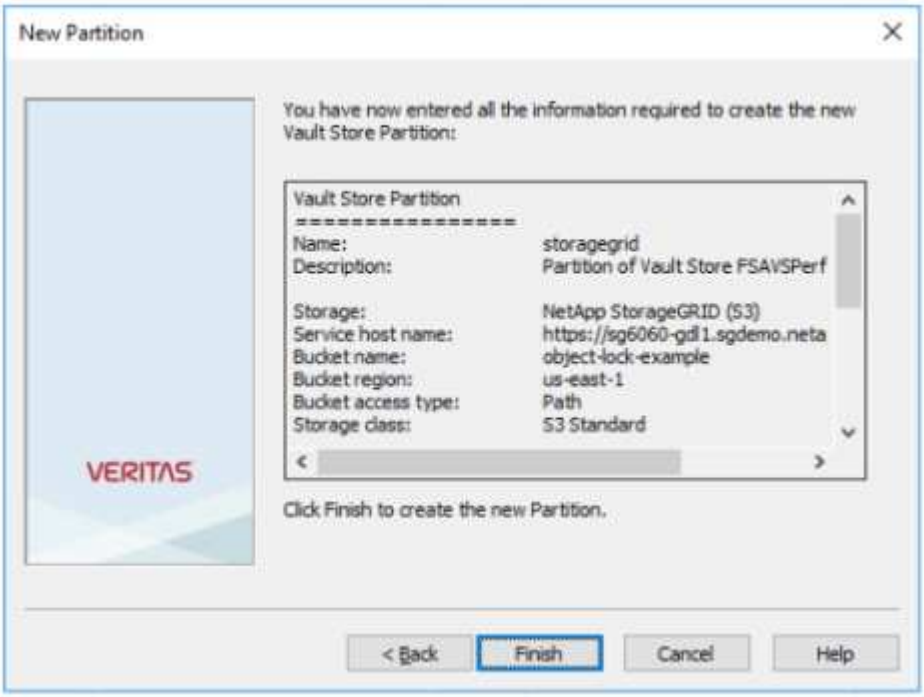


7. StorageGRID non supporta il parametro di replica S3. Per proteggere gli oggetti, StorageGRID utilizza le regole ILM (Information Lifecycle Management) per specificare schemi di protezione dei dati: Copie multiple o erasure coding. Selezionare l'opzione quando esistono file archiviati nell'archiviazione e fare clic

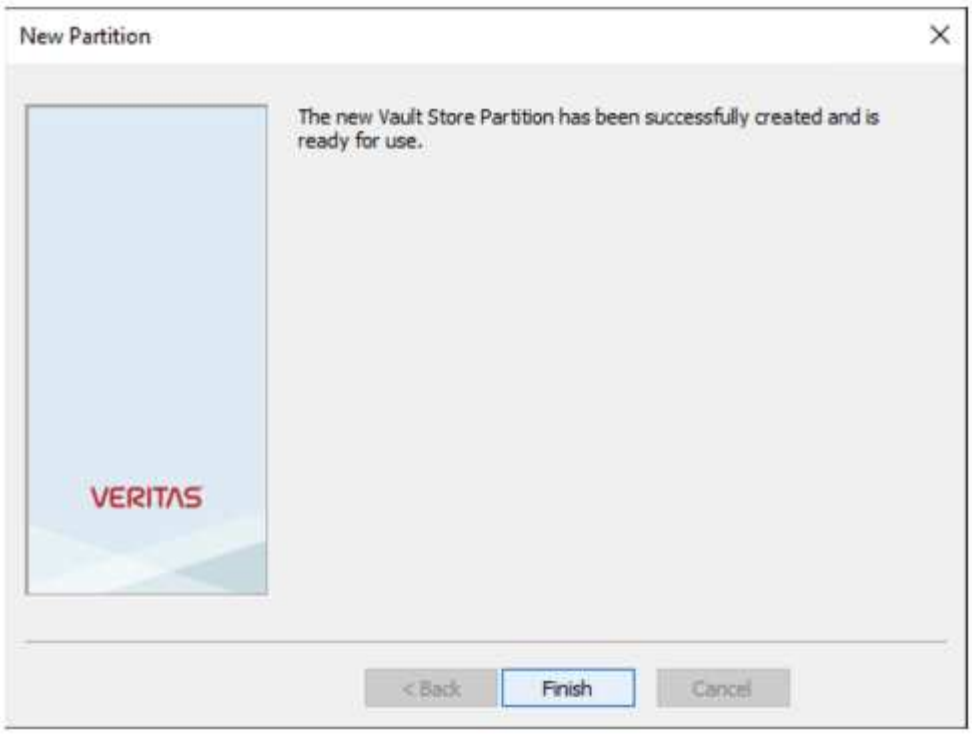
su Avanti.



8. Verificare le informazioni nella pagina di riepilogo e fare clic su fine.



9. Una volta creata la nuova partizione dell'archivio vault, è possibile archiviare, ripristinare e cercare i dati in Enterprise Vault con StorageGRID come storage primario.



Configurare il blocco degli oggetti StorageGRID S3 per lo storage WORM

Scopri come configurare StorageGRID per lo storage WORM utilizzando blocco oggetti S3.

Prerequisiti per configurare StorageGRID per lo storage WORM

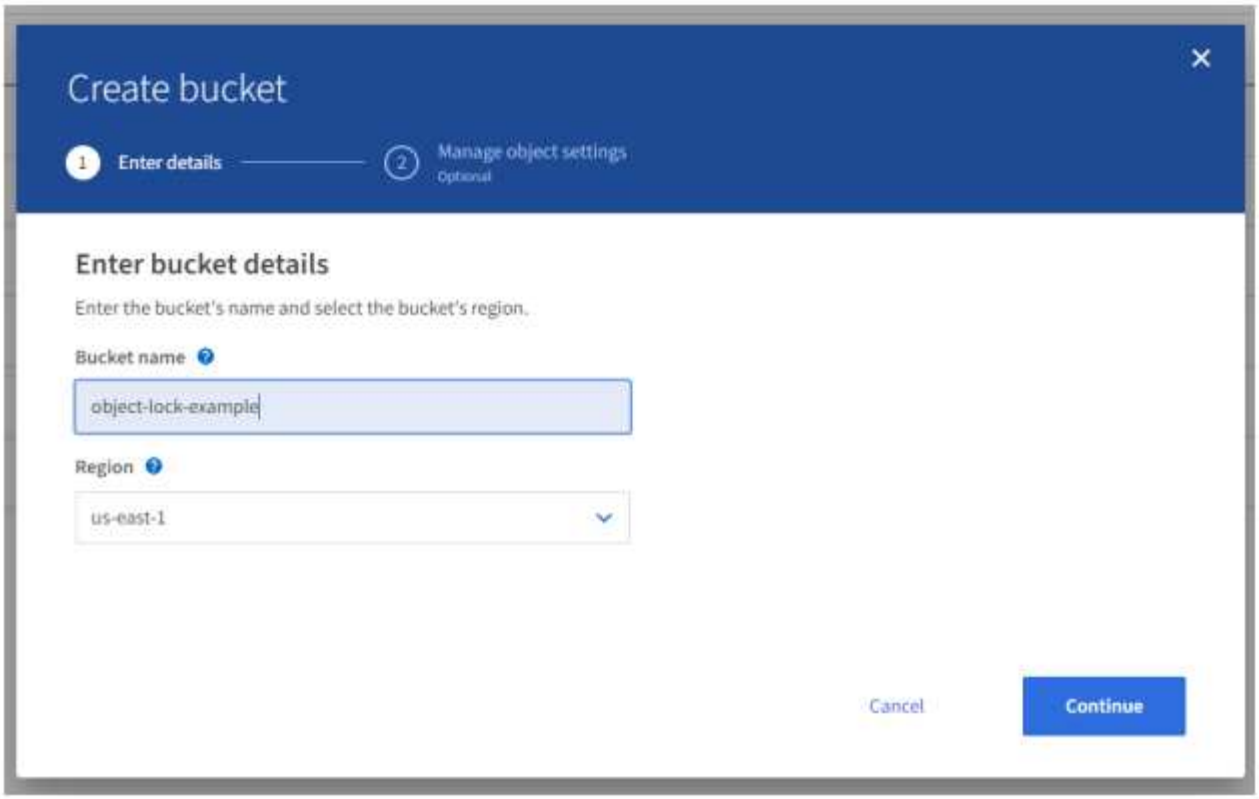
Per lo storage WORM, StorageGRID utilizza il blocco degli oggetti S3 per mantenere gli oggetti per la conformità. Ciò richiede StorageGRID 11,6 o superiore, in cui è stata introdotta la conservazione predefinita del bucket blocco oggetti S3. Enterprise Vault richiede anche la versione 14.2.2 o superiore.

Configurare la conservazione predefinita del bucket di blocco oggetti StorageGRID S3

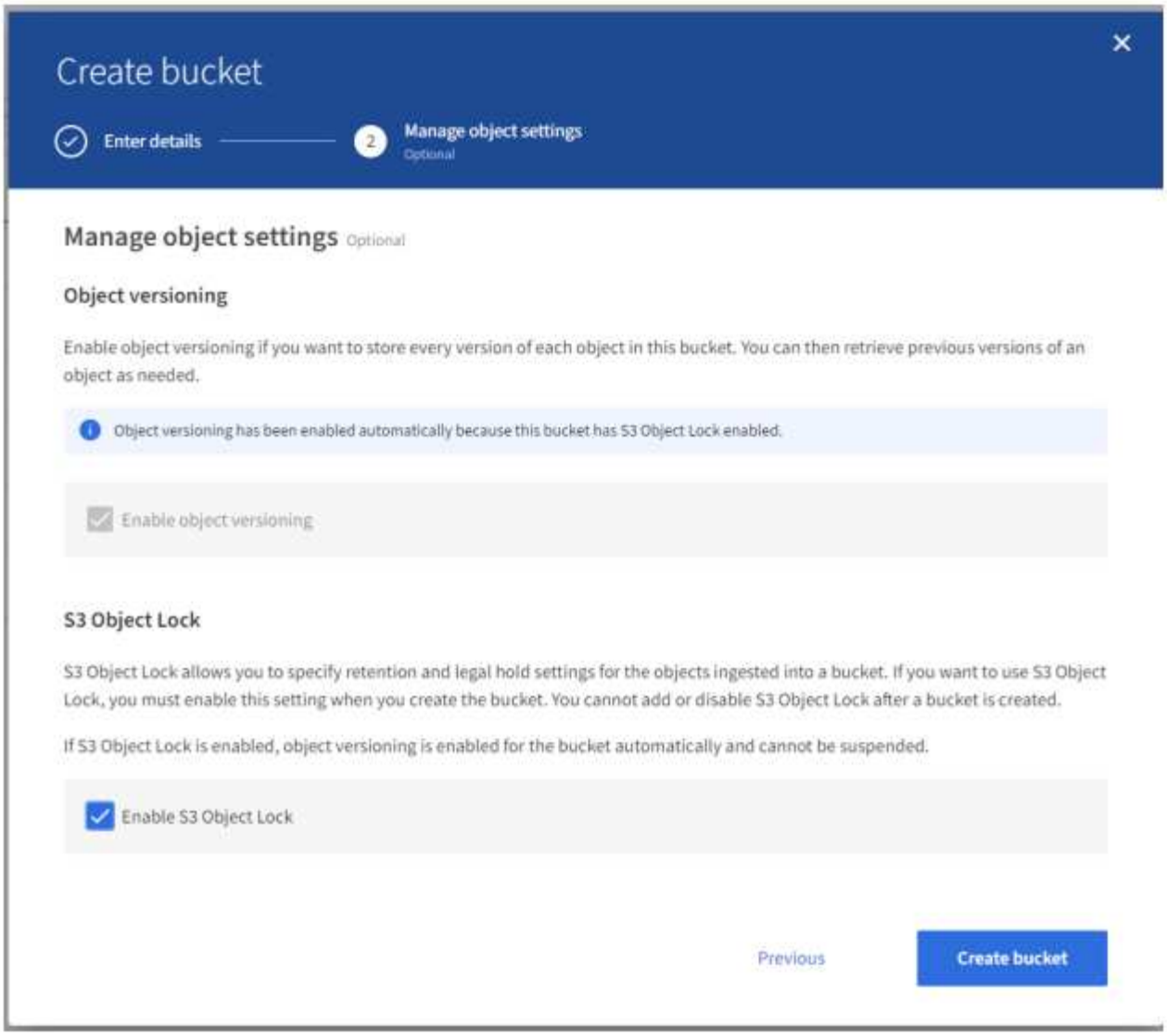
Per configurare la conservazione predefinita del bucket di blocco degli oggetti StorageGRID S3, attenersi alla seguente procedura:

Fasi

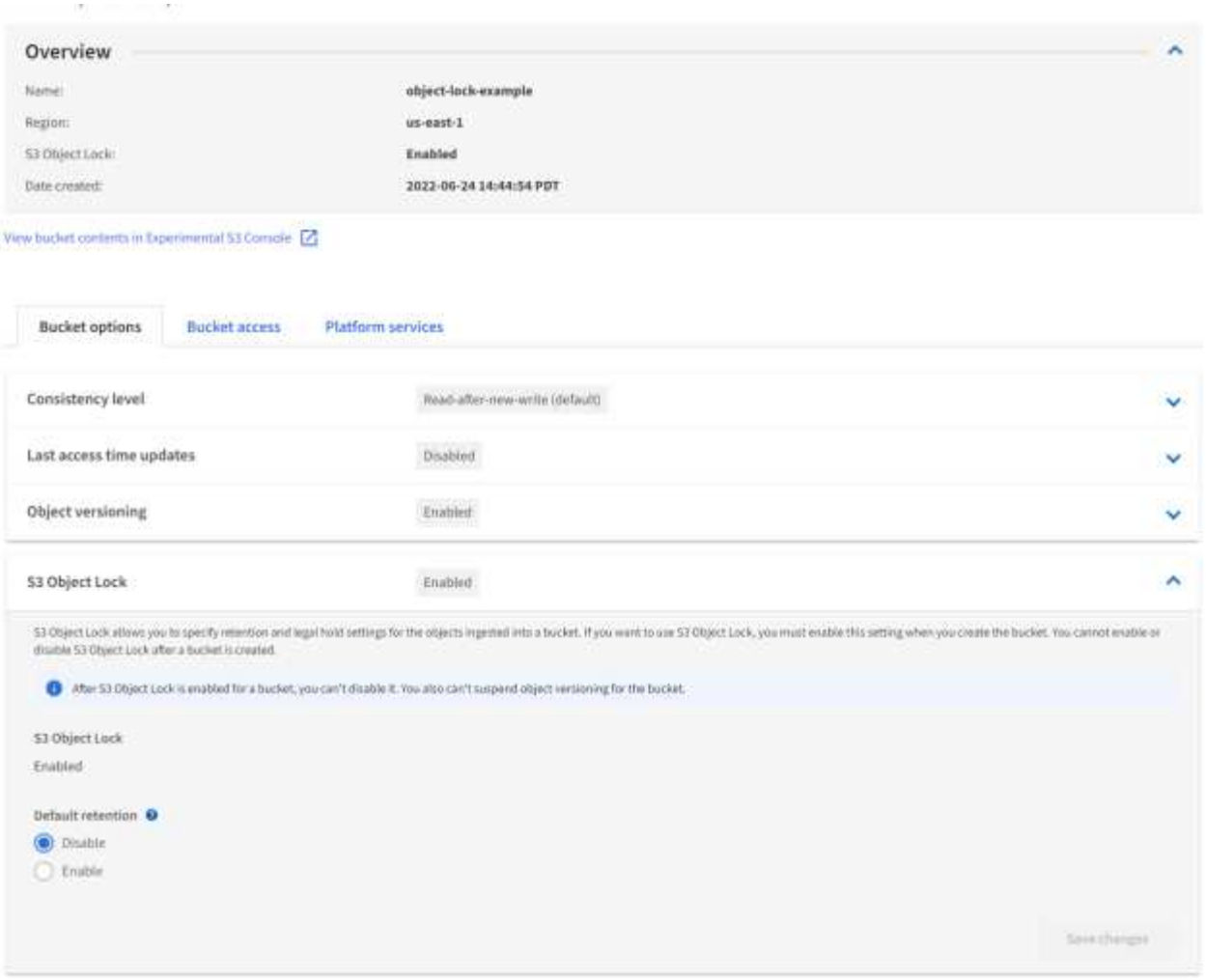
1. In Gestione tenant StorageGRID, creare un bucket e fare clic su continua



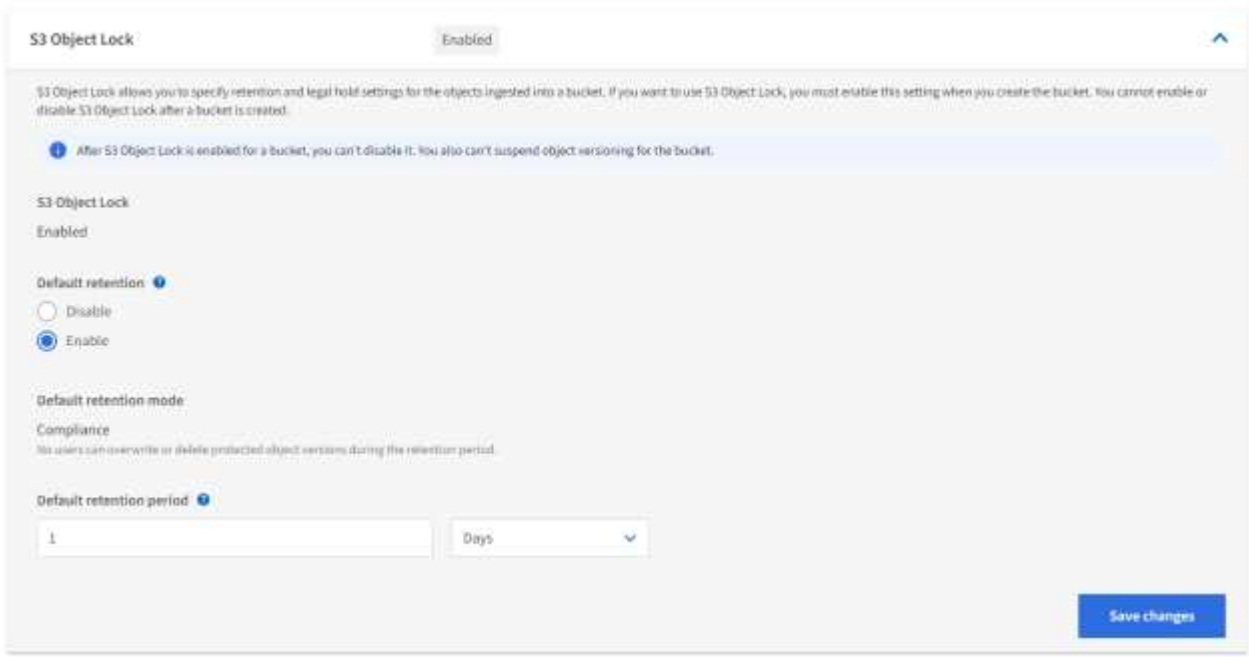
2. Selezionare l’opzione attiva blocco oggetti S3 e fare clic su Crea bucket.



3. Una volta creata la benna, selezionarla per visualizzare le opzioni della benna. Espandere l'opzione a discesa blocco oggetti S3.



4. In conservazione predefinita, selezionare attiva e impostare un periodo di conservazione predefinito di 1 giorno. Fare clic su Salva modifiche.



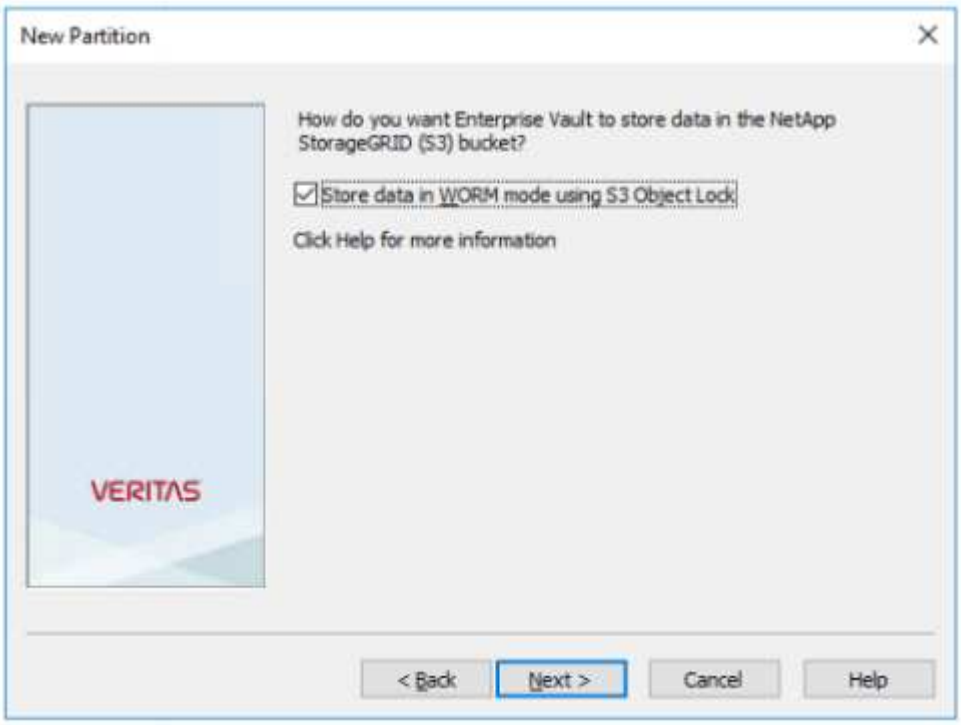
Il bucket è ora pronto per essere utilizzato da Enterprise Vault per memorizzare dati WORM.

Configurare Enterprise Vault

Per configurare Enterprise Vault, completare i seguenti passaggi:

Fasi

1. Ripetere i passaggi 1-3 della "Configurazione di base" sezione, ma questa volta selezionare l'opzione Memorizza dati in modalità WORM utilizzando blocco oggetti S3. Fare clic su Avanti.



2. Quando si immettono le impostazioni di connessione del bucket S3, assicurarsi di immettere il nome di un bucket S3 in cui è attivata la conservazione predefinita del blocco degli oggetti S3.
3. Verificare la connessione per verificare le impostazioni.

Configurare il failover del sito StorageGRID per il disaster recovery

Scoprite come configurare il failover del sito StorageGRID in uno scenario di disaster recovery.

È una prassi comune che l'implementazione di un'architettura StorageGRID sia multisito. I siti possono essere Active-Active o Active-passive per il disaster recovery. In uno scenario di disaster recovery, assicurati che veritas Enterprise Vault mantenga la connessione al proprio storage primario (StorageGRID) e continui ad acquisire e recuperare i dati durante un guasto del sito. In questa sezione vengono fornite istruzioni di configurazione di alto livello per una distribuzione attiva-passiva a due siti. Per informazioni dettagliate su queste linee guida, visitare "Documentazione StorageGRID" la pagina o contattare un esperto StorageGRID.

Prerequisiti per configurare StorageGRID con veritas Enterprise Vault

Prima di configurare il failover del sito StorageGRID, verificare i seguenti prerequisiti:

- È prevista una distribuzione di StorageGRID in due siti, ad esempio site1 e site2.
- È stato creato un nodo admin che esegue il servizio di bilanciamento del carico o un nodo gateway, in ciascun sito, per il bilanciamento del carico.
- È stato creato un endpoint di bilanciamento del carico StorageGRID.

Configurare il failover del sito StorageGRID

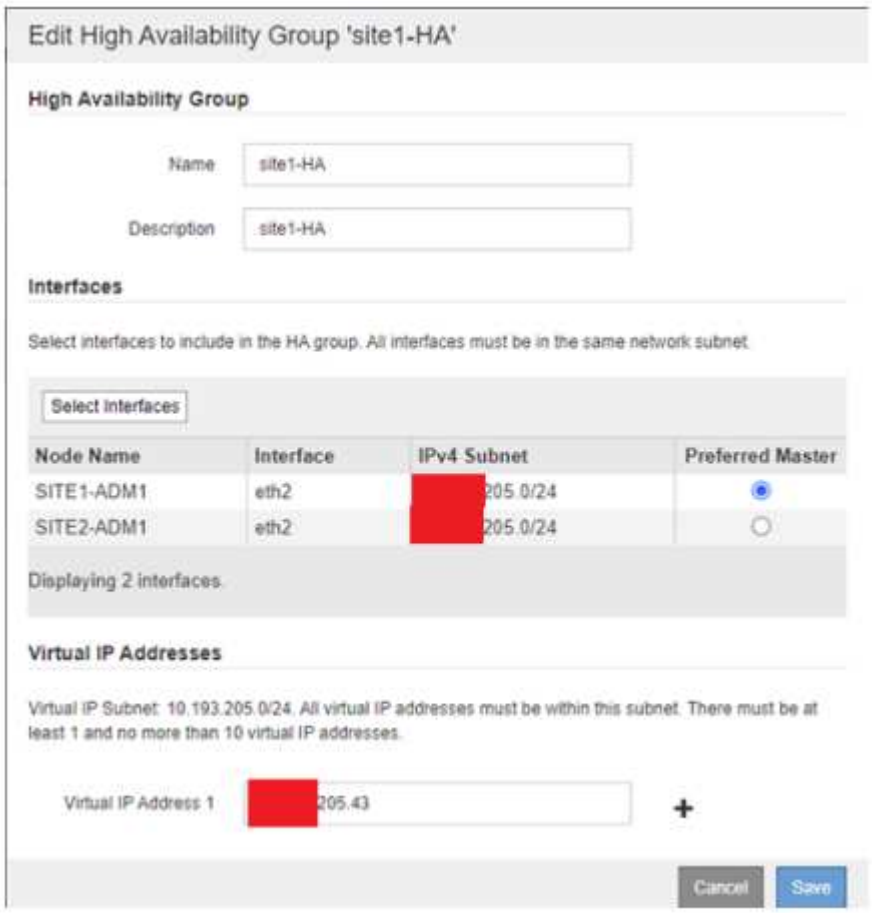
Per configurare il failover del sito StorageGRID, attenersi alla seguente procedura:

Fasi

1. Per garantire la connettività a StorageGRID in caso di guasti nel sito, configurare un gruppo ad alta disponibilità (ha). Dall'interfaccia GMI (StorageGRID Grid Manager Interface), fare clic su Configurazione, gruppi ad alta disponibilità e + Crea.

   [vertias/veritas-create-un-gruppo-ad-alta disponibilità]

2. Inserire le informazioni richieste. Fare clic su Select Interfaces (Seleziona interfacce) e includere le interfacce di rete di site1 e site2 in cui site1 (il sito primario) è il master preferito. Assegnare un indirizzo IP virtuale all'interno della stessa subnet. Fare clic su Salva.

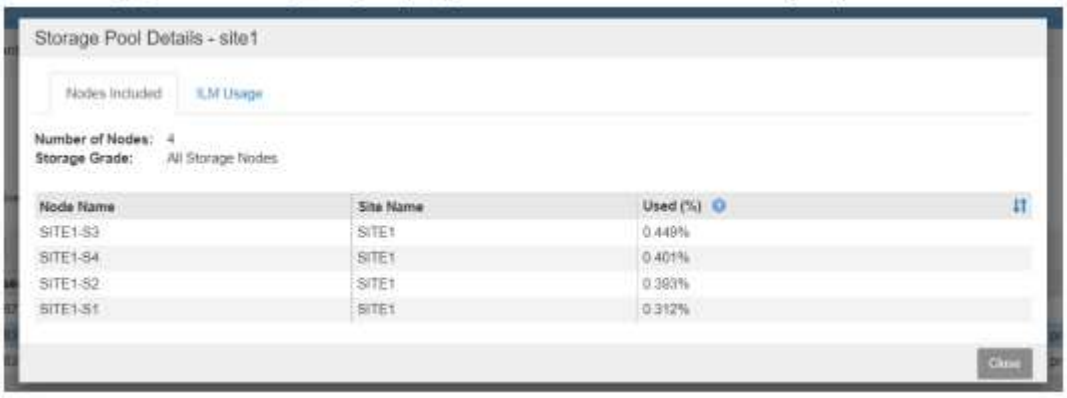


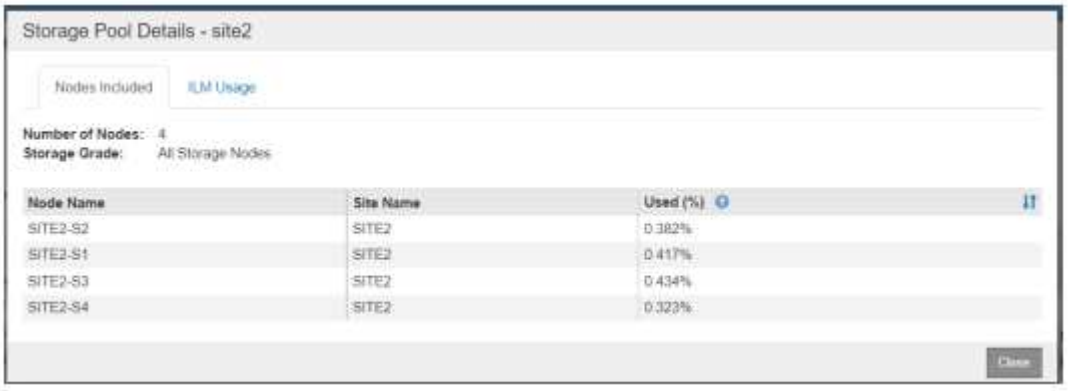
3. Questo indirizzo IP virtuale (VIP) deve essere associato al nome host S3 utilizzato durante la configurazione della partizione di veritas Enterprise Vault. L'indirizzo VIP risolve il traffico a site1 e, durante un errore site1, l'indirizzo VIP reindirizza il traffico a site2 in modo trasparente.
4. Verifica che i dati siano replicati su site1 e site2. In questo modo, se site1 fallisce, i dati dell'oggetto sono

ancora disponibili da site2. Questa operazione viene eseguita configurando per la prima volta i pool di storage.

Da StorageGRID GMI, fare clic su ILM, Storage Pools, quindi su + Crea. Seguire la procedura guidata per creare due pool di storage: Uno per site1 e uno per site2.

I pool di storage sono raggruppamenti logici di nodi utilizzati per definire il posizionamento degli oggetti





5. Da StorageGRID GMI, fare clic su ILM, regole, quindi su + Crea. Seguire la procedura guidata per creare una regola ILM specificando una copia da archiviare per sito con un comportamento di acquisizione bilanciato.

6. Aggiungere la regola ILM in un criterio ILM e attivare il criterio.

Questa configurazione produce i seguenti risultati:

- Un IP endpoint virtuale S3 in cui site1 è l'endpoint primario e site2 è l'endpoint secondario. Se site1

fallisce, il VIP passa a site2.

- Quando i dati archiviati vengono inviati da veritas Enterprise Vault, StorageGRID garantisce che una copia venga archiviata in site1 e un'altra copia di DR in site2. Se site1 si guasta, Enterprise Vault continua ad acquisire e recuperare da site2 TB.

> Entrambe queste configurazioni sono trasparenti per veritas Enterprise Vault. L'endpoint S3, il nome del bucket, le chiavi di accesso e così via sono gli stessi. Non è necessario riconfigurare le impostazioni di connessione S3 nella partizione veritas Enterprise Vault.