



Inizia subito

StorageGRID

NetApp
April 10, 2024

Sommario

- Inizia subito 1
 - Primer griglia 1
 - Linee guida per il networking 69

Inizia subito

Primer griglia

Grid primer: Panoramica

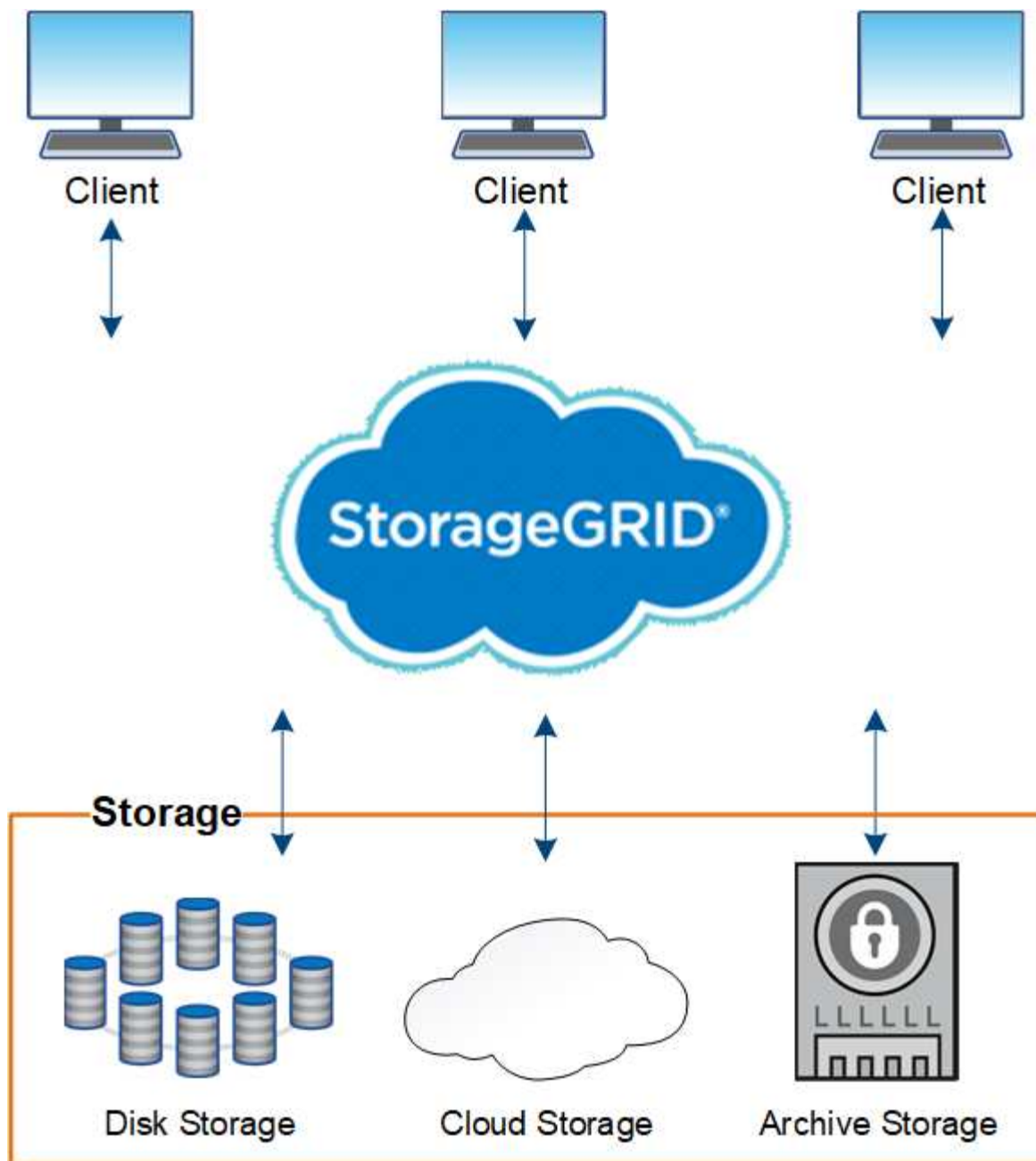
Utilizza questa introduzione per ottenere una panoramica del sistema StorageGRID e per scoprire l'architettura StorageGRID e la topologia di rete, le funzionalità di gestione dei dati e l'interfaccia utente.

Che cos'è 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 offre uno storage sicuro e durevole per i dati non strutturati su larga scala. Le policy integrate di gestione del ciclo di vita basate sui metadati ottimizzano la posizione dei dati durante l'intero ciclo di vita. I contenuti vengono posizionati nella giusta posizione, al momento giusto e nel giusto Tier di storage per ridurre i costi.

StorageGRID è composto da nodi eterogenei, ridondanti e distribuiti geograficamente, che possono essere integrati con le applicazioni client esistenti e di prossima generazione.



I vantaggi del sistema StorageGRID includono:

- Un repository di dati distribuito geograficamente per dati non strutturati, estremamente scalabile e facile da utilizzare.
- Protocolli standard di storage a oggetti:
 - Amazon Web Services Simple Storage Service (S3)
 - Swift di OpenStack
- Cloud ibrido abilitato. ILM (Information Lifecycle Management) basato su policy archivia gli oggetti nei cloud pubblici, tra cui Amazon Web Services (AWS) e Microsoft Azure. I servizi della piattaforma StorageGRID consentono la replica dei contenuti, la notifica degli eventi e la ricerca dei metadati degli oggetti archiviati nei cloud pubblici.
- Protezione flessibile dei dati per garantire durata e disponibilità. I dati possono essere protetti mediante replica e erasure coding a più livelli. La verifica dei dati a riposo e a bordo garantisce l'integrità per una

conservazione a lungo termine.

- Gestione dinamica del ciclo di vita dei dati per aiutare a gestire i costi dello storage. È possibile creare regole ILM per gestire il ciclo di vita dei dati a livello di oggetto e personalizzare la località dei dati, la durata, le performance, i costi e i tempi di conservazione. Il nastro è disponibile come Tier di archiviazione integrato.
- Elevata disponibilità dello storage dei dati e di alcune funzioni di gestione, con bilanciamento del carico integrato per ottimizzare il carico dei dati tra le risorse StorageGRID.
- Supporto di più account tenant di storage per separare gli oggetti memorizzati nel sistema da diverse entità.
- Numerosi strumenti per il monitoraggio dello stato di salute del sistema StorageGRID, tra cui un sistema di avviso completo, una dashboard grafica e stati dettagliati per tutti i nodi e i siti.
- Supporto per l'implementazione basata su software o hardware. È possibile implementare StorageGRID su uno dei seguenti sistemi:
 - Macchine virtuali in esecuzione in VMware.
 - Motori container su host Linux.
 - Appliances progettate da StorageGRID.
 - Le appliance di storage forniscono storage a oggetti.
 - Le appliance di servizi offrono servizi di gestione della griglia e bilanciamento del carico.
- Conforme ai requisiti di storage pertinenti delle seguenti normative:
 - Securities and Exchange Commission (SEC) in 17 cfr § 240.17a-4(f), che regola i membri di Exchange, gli intermediari o i rivenditori.
 - Financial Industry Regulatory Authority (FINRA) Rule 4511(c), che si difende ai requisiti di formato e supporti della norma SEC 17a-4(f).
 - Commodity Futures Trading Commission (CFTC) nel regolamento 17 cfr § 1.31(c)-(d), che regola il trading dei futures sulle commodity.
- Operazioni di upgrade e manutenzione senza interruzioni. Mantenere l'accesso ai contenuti durante le procedure di aggiornamento, espansione, decommissionamento e manutenzione.
- Gestione delle identità federate. Si integra con Active Directory, OpenLDAP o Oracle Directory Service per l'autenticazione degli utenti. Supporta SSO (Single Sign-on) utilizzando lo standard SAML 2.0 (Security Assertion Markup Language 2.0) per lo scambio di dati di autenticazione e autorizzazione tra StorageGRID e ad FS (Active Directory Federation Services).

Cloud ibridi con StorageGRID

Puoi utilizzare StorageGRID in una configurazione di cloud ibrido implementando la gestione dei dati basata su policy per memorizzare oggetti nei pool di storage cloud, sfruttando i servizi della piattaforma StorageGRID e spostando i dati su StorageGRID con NetApp FabricPool.

Pool di cloud storage

I pool di cloud storage consentono di memorizzare oggetti all'esterno del sistema StorageGRID. Ad esempio, è possibile spostare gli oggetti con accesso non frequente in uno storage cloud a basso costo, ad esempio Amazon S3 Glacier, S3 Glacier Deep Archive o il Tier di accesso all'archivio nello storage Microsoft Azure Blob. In alternativa, è possibile mantenere un backup cloud degli oggetti StorageGRID, che può essere utilizzato per ripristinare i dati persi a causa di un guasto di un volume di storage o di un nodo di storage.



L'utilizzo dei pool di storage cloud con FabricPool non è supportato a causa della latenza aggiunta per recuperare un oggetto dalla destinazione del pool di storage cloud.

Servizi della piattaforma S3

I servizi della piattaforma S3 consentono di utilizzare servizi remoti come endpoint per la replica di oggetti, le notifiche di eventi o l'integrazione della ricerca. I servizi della piattaforma operano indipendentemente dalle regole ILM della griglia e sono abilitati per i singoli bucket S3. Sono supportati i seguenti servizi:

- Il servizio di replica CloudMirror esegue automaticamente il mirroring di oggetti specifici in un bucket S3 di destinazione, che può essere su Amazon S3 o su un secondo sistema StorageGRID.
- Il servizio di notifica degli eventi invia messaggi relativi a azioni specifiche a un endpoint esterno che supporta la ricezione di eventi SNS (Simple Notification Service).
- Il servizio di integrazione della ricerca invia i metadati degli oggetti a un servizio esterno di Elasticsearch, consentendo la ricerca, la visualizzazione e l'analisi dei metadati mediante strumenti di terze parti.

Ad esempio, è possibile utilizzare la replica di CloudMirror per eseguire il mirroring di record specifici dei clienti in Amazon S3 e sfruttare i servizi AWS per eseguire analisi dei dati.

Tiering dei dati ONTAP con StorageGRID

È possibile ridurre il costo dello storage ONTAP mediante il tiering dei dati su StorageGRID con FabricPool. FabricPool è una tecnologia NetApp Data Fabric che consente il tiering automatizzato dei dati su Tier di storage a oggetti a basso costo, on-premise o off-premise.

A differenza delle soluzioni di tiering manuale, FabricPool riduce il costo totale di proprietà automatizzando il tiering dei dati per ridurre il costo dello storage. Offre i vantaggi dell'economia del cloud attraverso il tiering su cloud pubblici e privati, incluso StorageGRID.

Informazioni correlate

- [Amministrare StorageGRID](#)
- [Utilizzare un account tenant](#)
- [Gestire gli oggetti con ILM](#)
- [Configurare StorageGRID per FabricPool](#)

Architettura StorageGRID e topologia di rete

Un sistema StorageGRID è costituito da più tipi di nodi grid in uno o più siti del data center.

Per ulteriori informazioni sulla topologia della rete StorageGRID, sui requisiti e sulle comunicazioni Grid, consultare [Linee guida per il networking](#).

Topologie di implementazione

Il sistema StorageGRID può essere implementato in un singolo sito del data center o in più siti del data center.

Sito singolo

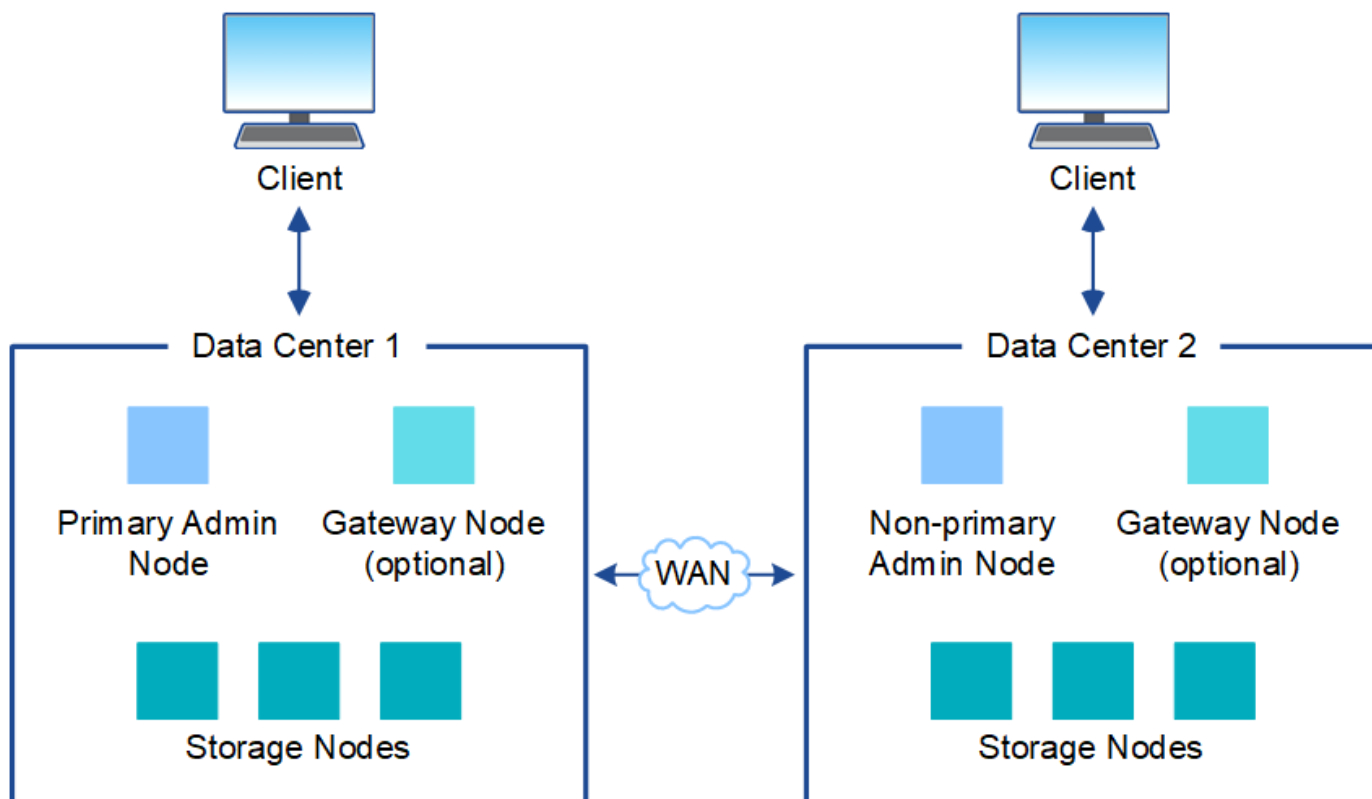
In un'implementazione con un singolo sito, l'infrastruttura e le operazioni del sistema StorageGRID sono centralizzate.



Più siti

In un'implementazione con più siti, è possibile installare diversi tipi e numeri di risorse StorageGRID in ogni sito. Ad esempio, potrebbe essere necessario più storage in un data center che in un altro.

Siti diversi sono spesso collocati in posizioni geografiche diverse in diversi domini di guasto, come ad esempio una linea di guasto sismica o una pianura alluvionale. La condivisione dei dati e il disaster recovery si ottengono attraverso la distribuzione automatica dei dati ad altri siti.



In un singolo data center possono inoltre esistere più siti logici per consentire l'utilizzo della replica distribuita e della codifica di cancellazione per aumentare la disponibilità e la resilienza.

Ridondanza del nodo di rete

In un'implementazione a sito singolo o multi-sito, è possibile includere facoltativamente più di un nodo di amministrazione o un nodo gateway per la ridondanza. Ad esempio, è possibile installare più di un nodo di amministrazione in un singolo sito o in diversi siti. Tuttavia, ogni sistema StorageGRID può disporre di un solo nodo amministratore primario.

Architettura di sistema

Questo diagramma mostra come i nodi della griglia sono disposti all'interno di un sistema StorageGRID.



I client S3 e Swift memorizzano e recuperano oggetti in StorageGRID. Altri client vengono utilizzati per inviare notifiche e-mail, per accedere all'interfaccia di gestione di StorageGRID e, facoltativamente, per accedere alla condivisione dell'audit.

I client S3 e Swift possono connettersi a un nodo gateway o a un nodo amministratore per utilizzare l'interfaccia di bilanciamento del carico per i nodi di storage. In alternativa, i client S3 e Swift possono connettersi direttamente ai nodi di storage utilizzando HTTPS.

Gli oggetti possono essere memorizzati all'interno di StorageGRID su nodi di storage basati su software o hardware, su supporti di archiviazione esterni come nastri o in pool di storage cloud, costituiti da bucket S3 esterni o container di storage Azure Blob.

Nodi e servizi Grid

Il building block di base di un sistema StorageGRID è il nodo grid. I nodi contengono servizi, ovvero moduli software che forniscono un insieme di funzionalità a un nodo grid.

Il sistema StorageGRID utilizza quattro tipi di nodi di rete:

- **I nodi di amministrazione** forniscono servizi di gestione quali configurazione, monitoraggio e registrazione del sistema. Quando si accede a Grid Manager, si sta effettuando la connessione a un nodo amministratore. Ogni grid deve avere un nodo di amministrazione primario e potrebbe avere ulteriori nodi di amministrazione non primari per la ridondanza. È possibile connettersi a qualsiasi nodo amministratore e ciascun nodo amministratore visualizza una vista simile del sistema StorageGRID. Tuttavia, le procedure di manutenzione devono essere eseguite utilizzando il nodo di amministrazione primario.

I nodi di amministrazione possono anche essere utilizzati per bilanciare il carico del traffico dei client S3 e Swift.

- **I nodi di storage** gestiscono e memorizzano i dati e i metadati degli oggetti. Ogni sistema StorageGRID deve avere almeno tre nodi di storage. Se si dispone di più siti, ogni sito all'interno del sistema StorageGRID deve avere anche tre nodi di storage.
- **I nodi gateway (opzionali)** forniscono un'interfaccia per il bilanciamento del carico che le applicazioni client possono utilizzare per connettersi a StorageGRID. Un bilanciamento del carico indirizza perfettamente i client a un nodo di storage ottimale, in modo che il guasto dei nodi o persino di un intero sito sia trasparente. È possibile utilizzare una combinazione di nodi gateway e nodi di amministrazione per il bilanciamento del carico oppure implementare un bilanciamento del carico HTTP di terze parti.
- **I nodi di archiviazione (opzionali)** forniscono un'interfaccia attraverso la quale i dati degli oggetti possono essere archiviati su nastro.

Per ulteriori informazioni, vedere [Amministrare StorageGRID](#).

Nodi basati su software

I nodi grid basati su software possono essere implementati nei seguenti modi:

- Come macchine virtuali (VM) in VMware vSphere
- All'interno di motori container su host Linux. Sono supportati i seguenti sistemi operativi:
 - Red Hat Enterprise Linux
 - CentOS
 - Ubuntu
 - Debian

Per ulteriori informazioni, vedere quanto segue:

- [Installare VMware](#)
- [Installare Red Hat Enterprise Linux o CentOS](#)
- [Installare Ubuntu o Debian](#)

Utilizzare "[Tool di matrice di interoperabilità NetApp](#)" per ottenere un elenco delle versioni supportate.

Nodi appliance StorageGRID

Le appliance hardware StorageGRID sono progettate appositamente per l'utilizzo in un sistema StorageGRID. Alcune appliance possono essere utilizzate come nodi di storage. Altri appliance possono essere utilizzati come nodi di amministrazione o nodi gateway. È possibile combinare nodi appliance con nodi basati su software o implementare grid all-appliance completamente progettati che non hanno dipendenze da hypervisor esterni, storage o hardware di calcolo.

Sono disponibili quattro tipi di appliance StorageGRID:

- Le appliance di servizi **SG100 e SG1000** sono server a 1 unità rack (1U) che possono funzionare ciascuno come nodo di amministrazione primario, nodo di amministrazione non primario o nodo gateway. Entrambe le appliance possono operare contemporaneamente come nodi gateway e nodi di amministrazione (primari e non primari).
- L'appliance di storage **SG6000** funziona come nodo di storage e combina il controller di calcolo 1U SG6000-CN con uno shelf di controller di storage 2U o 4U. SG6000 è disponibile in tre modelli:
 - **SGF6024**: Combina il controller di calcolo SG6000-CN con uno shelf di controller di storage 2U che include 24 unità a stato solido (SSD) e controller di storage ridondanti.
 - * **SG6060 e SG6060X**: Combina il controller di calcolo SG6000-CN con un enclosure 4U che include 58 unità NL-SAS, 2 SSD e controller storage ridondanti. SG6060 e SG6060X supportano ciascuno uno o due shelf di espansione da 60 dischi, fornendo fino a 178 dischi dedicati allo storage a oggetti.
- L'appliance di storage **SG5700** è una piattaforma di storage e calcolo integrata che opera come nodo di storage. SG5700 è disponibile in quattro modelli:
 - **SG5712 e SG5712X**: Enclosure 2U che include 12 unità NL-SAS e controller di calcolo e storage integrati.
 - **SG5760 e SG5760X**: Enclosure 4U che include 60 unità NL-SAS e controller di calcolo e storage integrati.
- L'appliance di storage **SG5600** è una piattaforma di storage e calcolo integrata che opera come nodo di storage. SG5600 è disponibile in due modelli:
 - **SG5612**: Enclosure 2U che include 12 unità NL-SAS e controller di calcolo e storage integrati.
 - **SG5660**: Enclosure 4U che include 60 unità NL-SAS e controller di calcolo e storage integrati.

Per ulteriori informazioni, vedere quanto segue:

- ["NetApp Hardware Universe"](#)
- [Appliance di servizi SG100 e SG1000](#)
- [Appliance di storage SG6000](#)
- [Appliance di storage SG5700](#)
- [Appliance di storage SG5600](#)

Servizi primari per nodi di amministrazione

La tabella seguente mostra i servizi primari per i nodi di amministrazione; tuttavia, questa tabella non elenca tutti i servizi dei nodi.

Servizio	Funzione dei tasti
Sistema di gestione dell'audit (AMS)	Tiene traccia dell'attività del sistema.
Nodo di gestione della configurazione (CMN)	Gestisce la configurazione a livello di sistema. Solo nodo amministratore primario.
Management Application Program Interface (Mgmt-api)	Elabora le richieste provenienti dall'API Grid Management e dall'API Tenant Management.
Alta disponibilità	Gestisce gli indirizzi IP virtuali ad alta disponibilità per gruppi di nodi di amministrazione e nodi gateway. Nota: questo servizio si trova anche sui nodi gateway.
Bilanciamento del carico	Fornisce il bilanciamento del carico del traffico S3 e Swift dai client ai nodi di storage. Nota: questo servizio si trova anche sui nodi gateway.
NMS (Network Management System)	Fornisce funzionalità per Grid Manager.
Prometheus	Raccoglie e memorizza le metriche.
Server Status Monitor (SSM)	Monitora il sistema operativo e l'hardware sottostante.

Servizi primari per i nodi di storage

La tabella seguente mostra i servizi primari per i nodi di storage; tuttavia, questa tabella non elenca tutti i servizi del nodo.



Alcuni servizi, come il servizio ADC e il servizio RSM, in genere esistono solo su tre nodi di storage in ogni sito.

Servizio	Funzione dei tasti
Account (acct)	Gestisce gli account tenant.
ADC (Administrative Domain Controller)	Mantiene la topologia e la configurazione a livello di griglia.
Cassandra	Memorizza e protegge i metadati degli oggetti.
Cassandra Reaper	Esegue la riparazione automatica dei metadati degli oggetti.
Chunk	Gestisce i dati con codifica erasure e i frammenti di parità.

Servizio	Funzione dei tasti
Data Mover (dmv)	Sposta i dati nei pool di cloud storage.
Data store distribuito (DDS)	Monitora lo storage dei metadati degli oggetti.
Identità (idnt)	Consente di federare le identità degli utenti da LDAP e Active Directory.
Router di distribuzione locale (LDR)	Elabora le richieste del protocollo di storage a oggetti e gestisce i dati degli oggetti su disco.
Replicated state Machine (RSM)	Garantisce che le richieste di servizio della piattaforma S3 vengano inviate ai rispettivi endpoint.
Server Status Monitor (SSM)	Monitora il sistema operativo e l'hardware sottostante.

Servizi primari per i nodi gateway

La tabella seguente mostra i servizi primari per i nodi gateway; tuttavia, questa tabella non elenca tutti i servizi dei nodi.

Servizio	Funzione dei tasti
Bilanciamento del carico di connessione (CLB)	Fornisce il bilanciamento del carico dei livelli 3 e 4 del traffico S3 e Swift dai client ai nodi di storage. Meccanismo di bilanciamento del carico legacy. Nota: il servizio CLB è obsoleto.
Alta disponibilità	Gestisce gli indirizzi IP virtuali ad alta disponibilità per gruppi di nodi di amministrazione e nodi gateway. Nota: questo servizio si trova anche nei nodi di amministrazione.
Bilanciamento del carico	Fornisce il bilanciamento del carico di livello 7 del traffico S3 e Swift dai client ai nodi di storage. Si tratta del meccanismo di bilanciamento del carico consigliato. Nota: questo servizio si trova anche nei nodi di amministrazione.
Server Status Monitor (SSM)	Monitora il sistema operativo e l'hardware sottostante.

Servizi primari per i nodi di archiviazione

La tabella seguente mostra i servizi primari per i nodi di archiviazione; tuttavia, questa tabella non elenca tutti i servizi dei nodi.

Servizio	Funzione dei tasti
Archivio (ARC)	Comunica con un sistema di storage su nastro esterno Tivoli Storage Manager (TSM).
Server Status Monitor (SSM)	Monitora il sistema operativo e l'hardware sottostante.

Servizi StorageGRID

Di seguito viene riportato un elenco completo dei servizi StorageGRID.

- **Account Service Forwarder**

Fornisce un'interfaccia per il servizio Load Balancer per eseguire query sull'account Service sugli host remoti e fornisce notifiche delle modifiche della configurazione degli endpoint del bilanciamento del carico al servizio Load Balancer. Il servizio Load Balancer è presente nei nodi Admin e nei nodi Gateway.

- **Servizio ADC (Controller di dominio amministrativo)**

Mantiene le informazioni sulla topologia, fornisce servizi di autenticazione e risponde alle query provenienti dai servizi LDR e CMN. Il servizio ADC è presente su ciascuno dei primi tre nodi di storage installati in un sito.

- **Servizio AMS (Audit Management System)**

Monitora e registra tutti gli eventi e le transazioni di sistema verificati in un file di log di testo. Il servizio AMS è presente nei nodi di amministrazione.

- **Servizio ARC (Archivio)**

Fornisce l'interfaccia di gestione con cui configurare le connessioni allo storage di archiviazione esterno, ad esempio il cloud tramite un'interfaccia S3 o un nastro tramite il middleware TSM. Il servizio ARC è presente nei nodi di archiviazione.

- **Cassandra Reaper service**

Esegue la riparazione automatica dei metadati degli oggetti. Il servizio Cassandra Reaper è presente su tutti i nodi di storage.

- **Servizio Chunk**

Gestisce i dati con codifica erasure e i frammenti di parità. Il servizio Chunk è presente sui nodi di storage.

- **Servizio CLB (bilanciamento del carico di connessione)**

Servizio obsoleto che fornisce un gateway in StorageGRID per le applicazioni client che si connettono tramite HTTP. Il servizio CLB è presente sui nodi gateway. Il servizio CLB è obsoleto e verrà rimosso in una release futura di StorageGRID.

- **Servizio CMN (nodo di gestione della configurazione)**

Gestisce le configurazioni a livello di sistema e le attività di grid. Ogni griglia dispone di un servizio CMN, presente sul nodo di amministrazione primario.

- **Servizio DDS (archivio dati distribuito)**

Si interfaccia con il database Cassandra per gestire i metadati degli oggetti. Il servizio DDS è presente sui nodi di storage.

- **Servizio DMV (Data Mover)**

Sposta i dati negli endpoint cloud. Il servizio DMV è presente sui nodi di storage.

- **Servizio IP dinamico**

Monitora la griglia per verificare la presenza di modifiche IP dinamiche e aggiorna le configurazioni locali. Il servizio Dynamic IP (dinip) è presente su tutti i nodi.

- **Servizio Grafana**

Utilizzato per la visualizzazione delle metriche in Grid Manager. Il servizio Grafana è presente nei nodi di amministrazione.

- **Servizio ad alta disponibilità**

Gestisce gli IP virtuali ad alta disponibilità sui nodi configurati nella pagina High Availability Groups. Il servizio High Availability è presente nei nodi Admin e nei nodi Gateway. Questo servizio è anche noto come servizio keepalived.

- **Servizio identità (idnt)**

Consente di federare le identità degli utenti da LDAP e Active Directory. Il servizio di identità (idnt) è presente su tre nodi di storage in ogni sito.

- **Servizio arbitro Lambda**

Gestisce le richieste S3 Select SelectObjectContent.

- **Servizio Load Balancer**

Fornisce il bilanciamento del carico del traffico S3 e Swift dai client ai nodi di storage. Il servizio Load Balancer può essere configurato tramite la pagina di configurazione degli endpoint del bilanciamento del carico. Il servizio Load Balancer è presente nei nodi Admin e nei nodi Gateway. Questo servizio è noto anche come servizio nginx-gw.

- **Servizio LDR (Local Distribution Router)**

Gestisce lo storage e il trasferimento dei contenuti all'interno della griglia. Il servizio LDR è presente sui nodi di storage.

- **Servizio MISCd Information Service Control Daemon**

Fornisce un'interfaccia per eseguire query e gestire servizi su altri nodi e per gestire le configurazioni ambientali sul nodo, ad esempio per eseguire query sullo stato dei servizi in esecuzione su altri nodi. Il servizio MISCd è presente su tutti i nodi.

- **servizio nginx**

Agisce come meccanismo di autenticazione e comunicazione sicura per diversi servizi grid (come Prometheus e Dynamic IP) per poter comunicare con servizi su altri nodi tramite API HTTPS. Il servizio

nginx è presente su tutti i nodi.

- **servizio nginx-gw**

Alimenta il servizio Load Balancer. Il servizio nginx-gw è presente nei nodi Admin e nei nodi Gateway.

- **Servizio NMS (Network Management System)**

Alimenta le opzioni di monitoraggio, reporting e configurazione visualizzate tramite Grid Manager. Il servizio NMS è presente nei nodi di amministrazione.

- **Servizio di persistenza**

Gestisce i file sul disco root che devono persistere durante un riavvio. Il servizio di persistenza è presente su tutti i nodi.

- **Servizio Prometheus**

Raccoglie le metriche delle serie temporali dai servizi su tutti i nodi. Il servizio Prometheus è presente sui nodi di amministrazione.

- **Servizio RSM (Replicated state Machine Service)**

Garantisce che le richieste di servizio della piattaforma vengano inviate ai rispettivi endpoint. Il servizio RSM è presente sui nodi di storage che utilizzano il servizio ADC.

- **Servizio SSM (Server Status Monitor)**

Monitora le condizioni dell'hardware e invia report al servizio NMS. Un'istanza del servizio SSM è presente su ogni nodo grid.

- **Servizio di raccolta tracce**

Esegue la raccolta di tracce per raccogliere informazioni da utilizzare per il supporto tecnico. Il servizio trace collector utilizza il software Jaeger open source ed è presente sui nodi di amministrazione.

Gestione degli oggetti

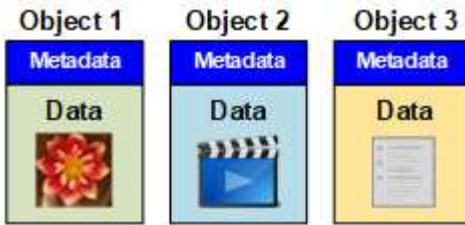
Come StorageGRID gestisce i dati

Quando si inizia a lavorare con il sistema StorageGRID, è utile comprendere come il sistema StorageGRID gestisce i dati.

Che cos'è un oggetto

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

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



Dati dell'oggetto

I dati degli oggetti possono essere qualsiasi cosa, ad esempio una fotografia, un filmato o un documento medico.

Metadati dell'oggetto

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

I metadati dell'oggetto includono informazioni come:

- Metadati di sistema, tra cui un ID univoco per ciascun oggetto (UUID), il nome dell'oggetto, il nome del bucket S3 o del container Swift, il nome o l'ID dell'account tenant, la dimensione logica dell'oggetto, la data e l'ora in cui l'oggetto è stato creato per la prima volta, e la data e l'ora dell'ultima modifica dell'oggetto.
- La posizione di storage corrente di ogni copia di oggetto o frammento con codifica di cancellazione.
- Qualsiasi metadati utente associato all'oggetto.

I metadati degli oggetti sono personalizzabili ed espandibili, il che lo rende flessibile per l'utilizzo da parte delle applicazioni.

Per informazioni dettagliate su come e dove StorageGRID memorizza i metadati degli oggetti, visitare il sito [Gestire lo storage dei metadati degli oggetti](#).

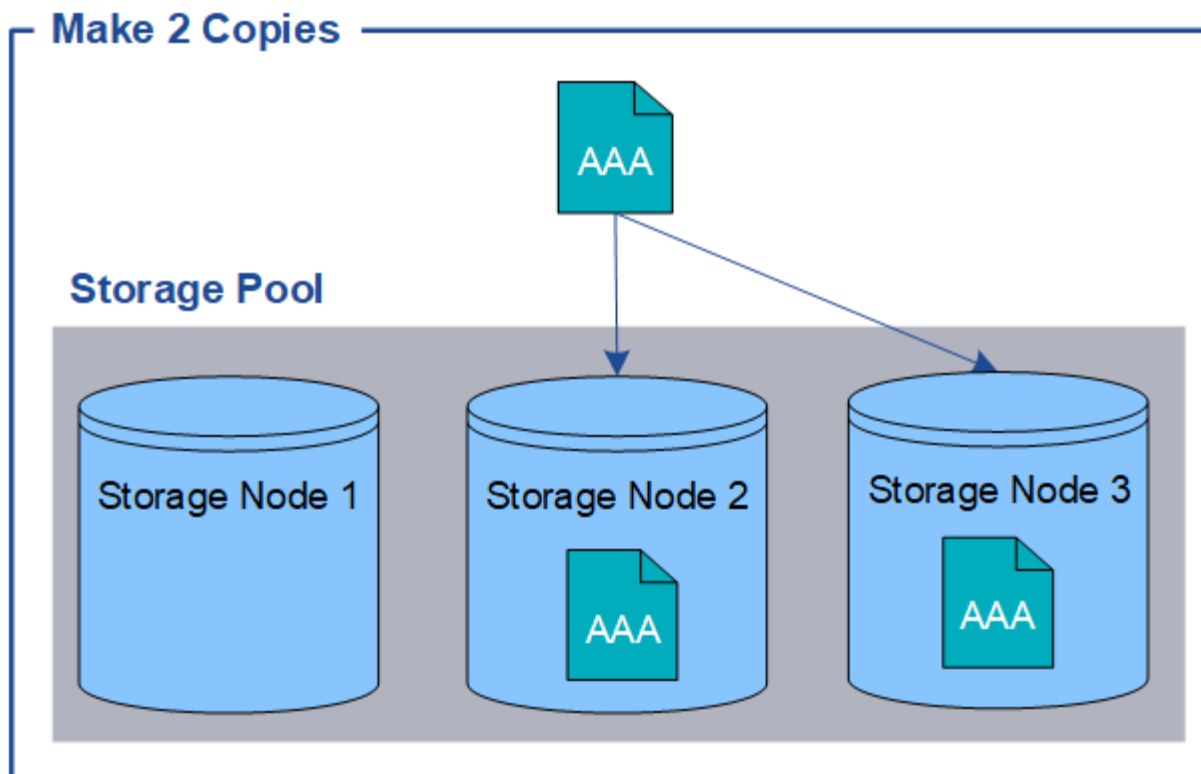
Modalità di protezione dei dati degli oggetti

Il sistema StorageGRID offre due meccanismi per proteggere i dati degli oggetti dalla perdita: Replica e erasure coding.

Replica

Quando StorageGRID associa gli oggetti a una regola ILM (Information Lifecycle Management) configurata per creare copie replicate, il sistema crea copie esatte dei dati degli oggetti e li memorizza nei nodi di storage, nei nodi di archivio o nei pool di storage cloud. Le regole ILM determinano il numero di copie effettuate, la posizione in cui vengono memorizzate e la durata della conservazione da parte del sistema. Se una copia viene persa, ad esempio, a causa della perdita di un nodo di storage, l'oggetto rimane disponibile se una copia di esso esiste altrove nel sistema StorageGRID.

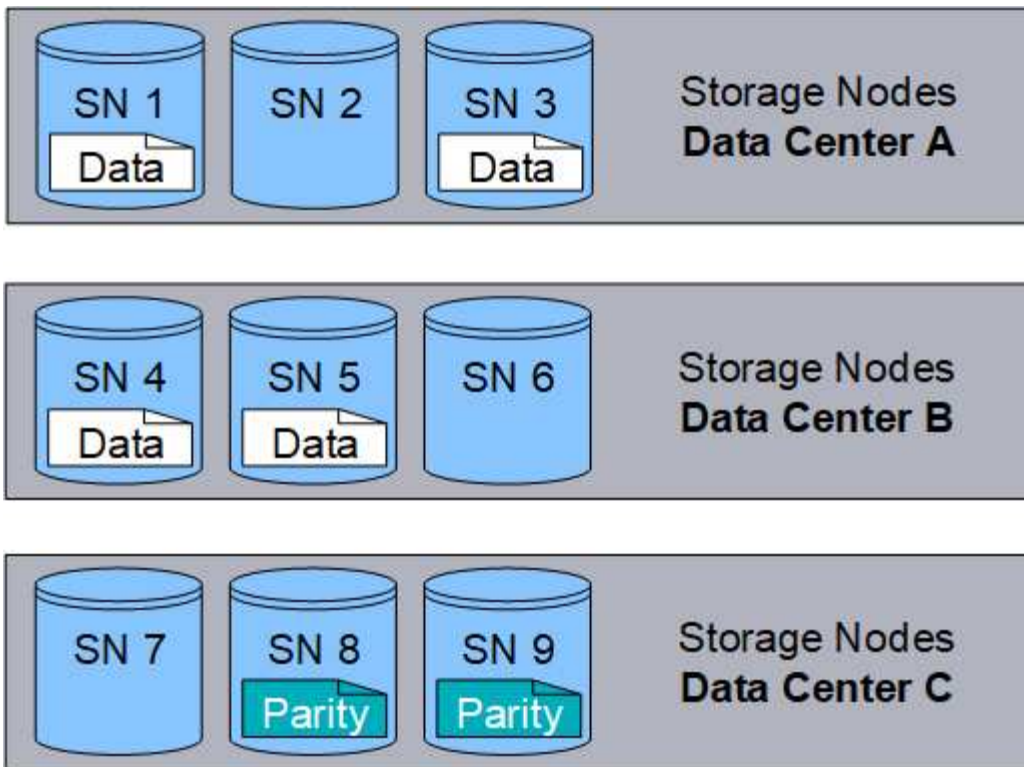
Nell'esempio seguente, la regola Make 2 copies specifica che due copie replicate di ciascun oggetto devono essere collocate in un pool di storage che contiene tre nodi di storage.



Erasure coding

Quando StorageGRID associa oggetti a una regola ILM configurata per creare copie con codifica di cancellazione, slice i dati degli oggetti in frammenti di dati, calcola ulteriori frammenti di parità e memorizza ogni frammento su un nodo di storage diverso. Quando si accede a un oggetto, questo viene riassembleato utilizzando i frammenti memorizzati. Se un dato o un frammento di parità viene corrotto o perso, l'algoritmo di erasure coding può ricreare quel frammento utilizzando un sottoinsieme dei rimanenti dati e frammenti di parità. Le regole ILM e i profili di erasure coding determinano lo schema di erasure coding utilizzato.

Nell'esempio riportato di seguito viene illustrato l'utilizzo della codifica erasure sui dati di un oggetto. In questo esempio, la regola ILM utilizza uno schema di erasure coding 4+2. Ciascun oggetto viene suddiviso in quattro frammenti di dati uguali e due frammenti di parità vengono calcolati dai dati dell'oggetto. Ciascuno dei sei frammenti viene memorizzato su un nodo di storage diverso in tre data center per fornire protezione dei dati in caso di guasti al nodo o perdita del sito.



Informazioni correlate

- [Gestire gli oggetti con ILM](#)
- [Utilizza la gestione del ciclo di vita delle informazioni](#)

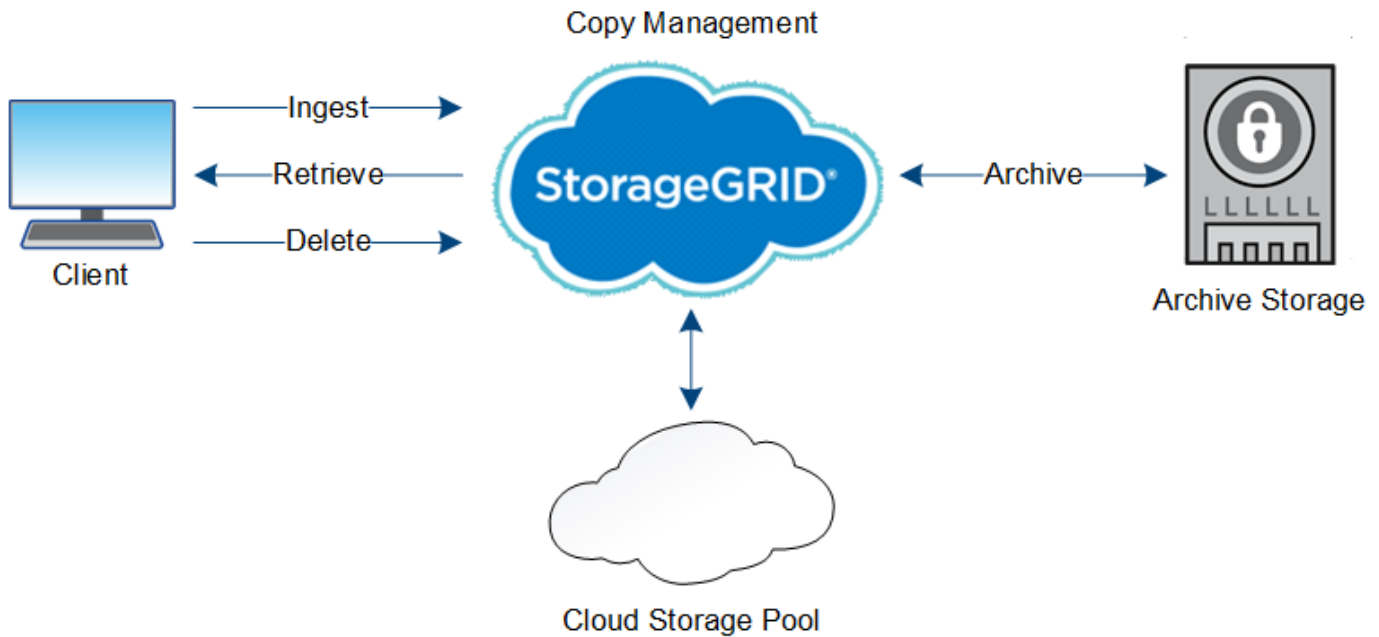
Ciclo di vita degli oggetti

La vita di un oggetto

La vita di un oggetto è costituita da varie fasi. Ogni fase rappresenta le operazioni che avvengono con l'oggetto.

La durata di un oggetto include le operazioni di acquisizione, gestione delle copie, recupero ed eliminazione.

- **Ingest:** Il processo di un'applicazione client S3 o Swift che salva un oggetto su HTTP nel sistema StorageGRID. In questa fase, il sistema StorageGRID inizia a gestire l'oggetto.
- **Gestione delle copie:** Processo di gestione delle copie replicate e codificate in cancellazione in StorageGRID, come descritto dalle regole ILM nella policy ILM attiva. Durante la fase di gestione delle copie, StorageGRID protegge i dati degli oggetti dalla perdita creando e mantenendo il numero e il tipo specificati di copie degli oggetti nei nodi di storage, in un pool di storage cloud o nel nodo di archiviazione.
- **Recupera:** Il processo di accesso di un'applicazione client a un oggetto memorizzato dal sistema StorageGRID. Il client legge l'oggetto, che viene recuperato da un nodo di storage, un pool di storage cloud o un nodo di archivio.
- **Delete:** Processo di rimozione di tutte le copie di oggetti dalla griglia. Gli oggetti possono essere eliminati in seguito all'invio da parte dell'applicazione client di una richiesta di eliminazione al sistema StorageGRID o in seguito a un processo automatico eseguito da StorageGRID alla scadenza della vita dell'oggetto.



Informazioni correlate

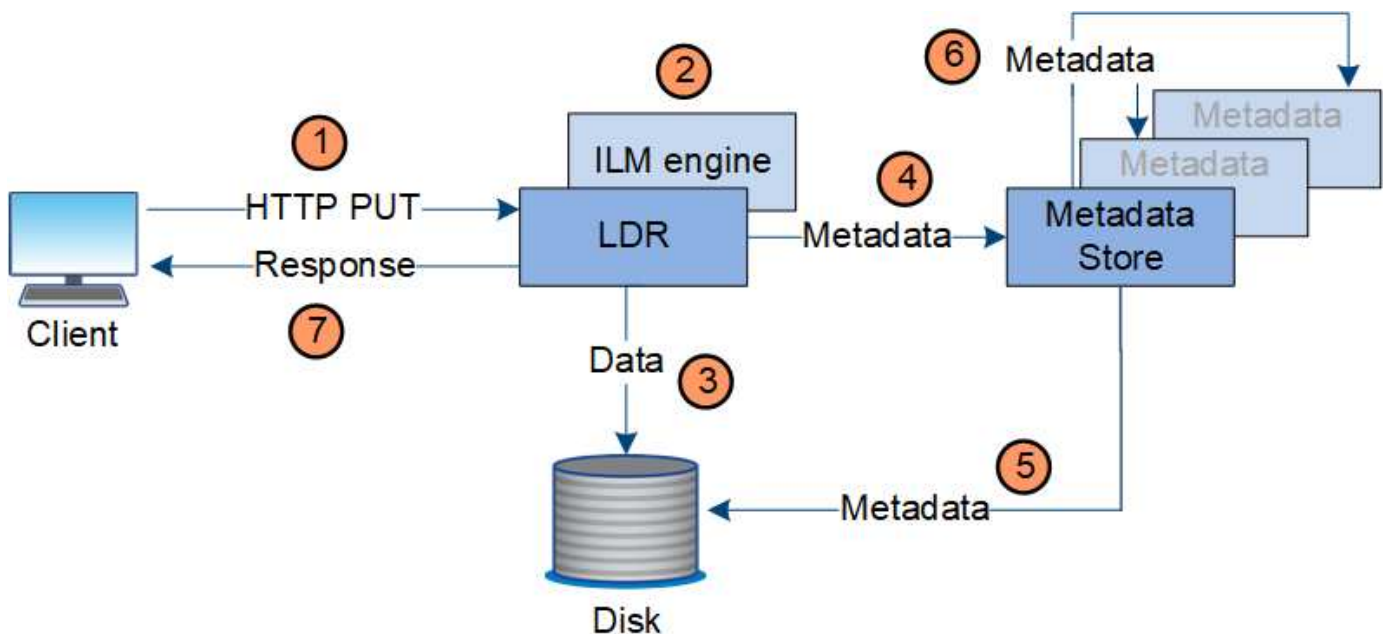
- [Gestire gli oggetti con ILM](#)
- [Utilizza la gestione del ciclo di vita delle informazioni](#)

Acquisire il flusso di dati

Un'operazione di acquisizione, o salvataggio, consiste in un flusso di dati definito tra il client e il sistema StorageGRID.

Flusso di dati

Quando un client acquisisce un oggetto nel sistema StorageGRID, il servizio LDR sui nodi di storage elabora la richiesta e memorizza i metadati e i dati su disco.



1. L'applicazione client crea l'oggetto e lo invia al sistema StorageGRID tramite una richiesta HTTP PUT.
2. L'oggetto viene valutato in base al criterio ILM del sistema.
3. Il servizio LDR salva i dati dell'oggetto come copia replicata o come copia codificata in cancellazione. (Il diagramma mostra una versione semplificata della memorizzazione di una copia replicata su disco).
4. Il servizio LDR invia i metadati dell'oggetto all'archivio di metadati.
5. L'archivio di metadati salva i metadati dell'oggetto su disco.
6. L'archivio di metadati propaga le copie dei metadati degli oggetti ad altri nodi di storage. Queste copie vengono salvate anche su disco.
7. Il servizio LDR restituisce una risposta HTTP 200 OK al client per confermare che l'oggetto è stato acquisito.

Gestione delle copie

I dati degli oggetti vengono gestiti dal criterio ILM attivo e dalle relative regole ILM. Le regole ILM effettuano copie replicate o erasure coded per proteggere i dati degli oggetti dalla perdita.

Potrebbero essere necessari diversi tipi o posizioni di copie di oggetti in momenti diversi della vita dell'oggetto. Le regole ILM vengono periodicamente valutate per garantire che gli oggetti vengano posizionati come richiesto.

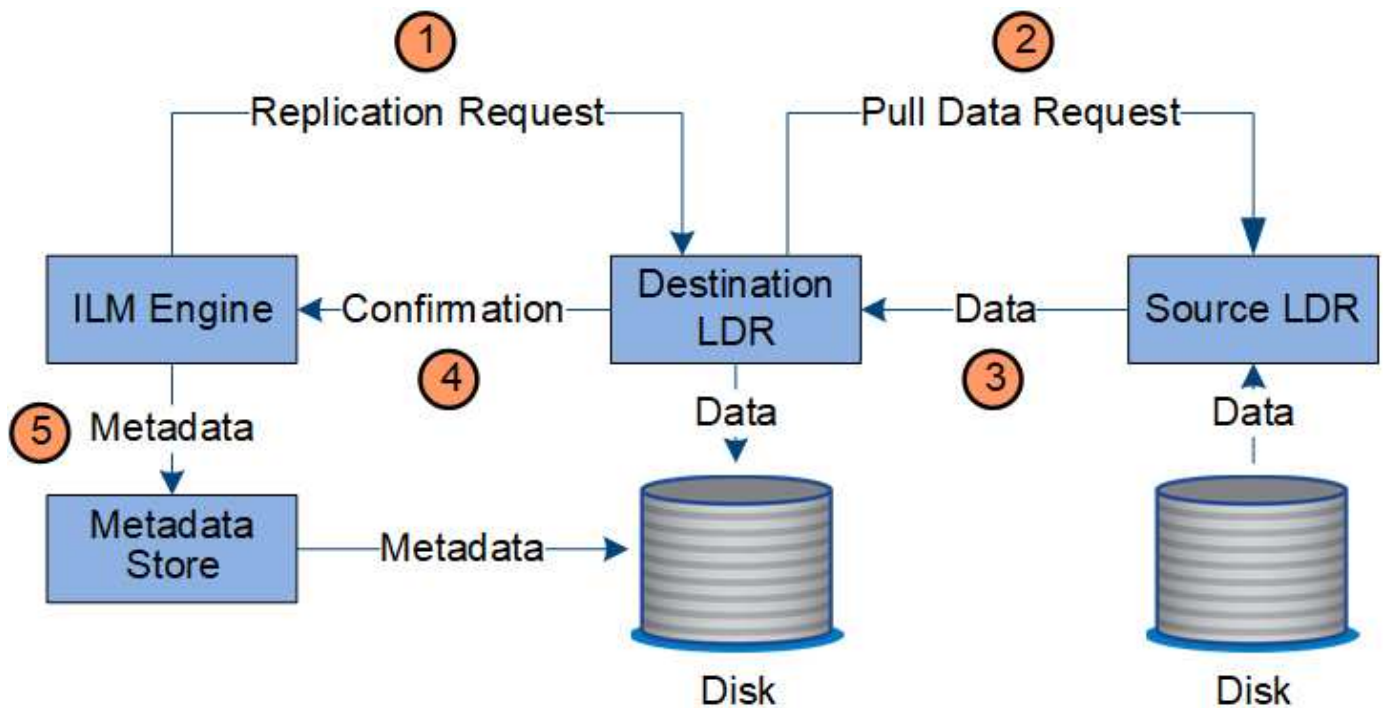
I dati degli oggetti vengono gestiti dal servizio LDR.

Protezione del contenuto: Replica

Se le istruzioni di posizionamento del contenuto di una regola ILM richiedono copie replicate dei dati dell'oggetto, le copie vengono eseguite e memorizzate su disco dai nodi di storage che compongono il pool di storage configurato.

Flusso di dati

Il motore ILM nel servizio LDR controlla la replica e garantisce che il numero corretto di copie venga memorizzato nelle posizioni corrette e per il tempo corretto.



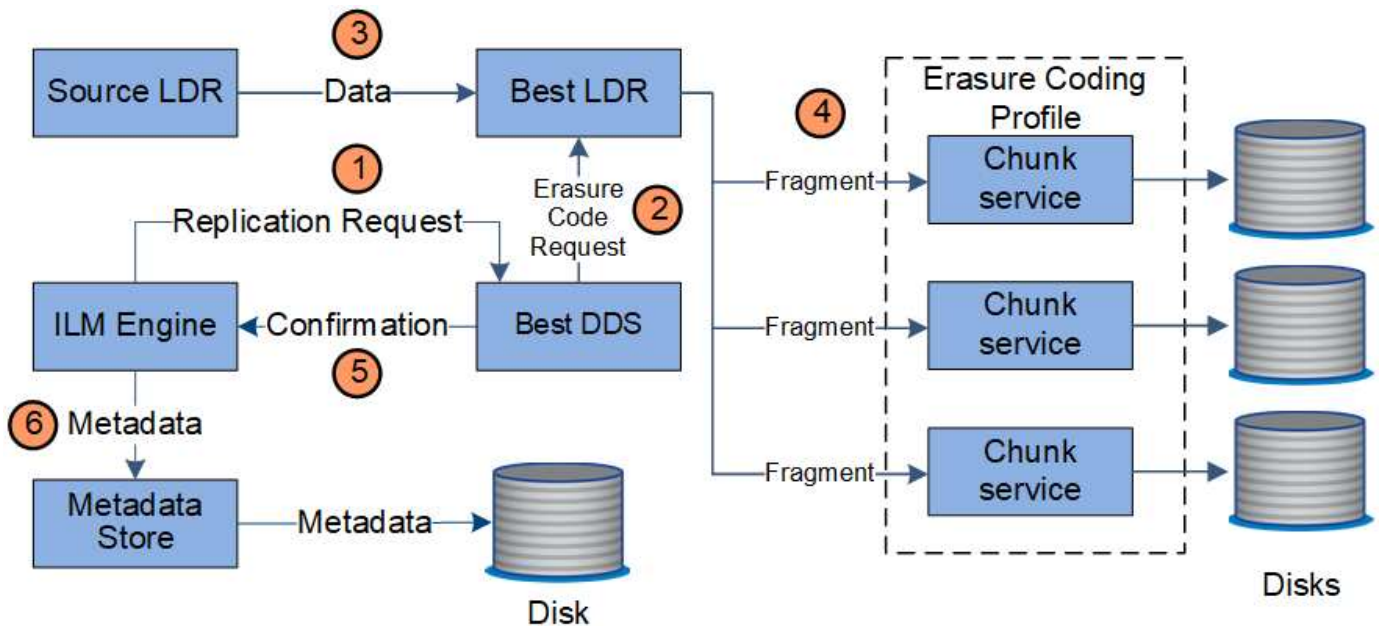
1. Il motore ILM interroga il servizio ADC per determinare il servizio LDR di destinazione migliore all'interno del pool di storage specificato dalla regola ILM. Quindi, invia al servizio LDR un comando per avviare la replica.
2. Il servizio LDR di destinazione interroga il servizio ADC per la migliore posizione di origine. Quindi, invia una richiesta di replica al servizio LDR di origine.
3. Il servizio LDR di origine invia una copia al servizio LDR di destinazione.
4. Il servizio LDR di destinazione notifica al motore ILM che i dati dell'oggetto sono stati memorizzati.
5. Il motore ILM aggiorna l'archivio di metadati con i metadati della posizione dell'oggetto.

Protezione del contenuto: Erasure coding

Se una regola ILM include istruzioni per eseguire copie codificate di cancellazione dei dati dell'oggetto, lo schema di erasure coding applicabile suddivide i dati dell'oggetto in dati e frammenti di parità e distribuisce tali frammenti tra i nodi di storage configurati nel profilo di codifica Erasure.

Flusso di dati

Il motore ILM, che è un componente del servizio LDR, controlla la codifica di cancellazione e garantisce che il profilo di codifica Erasure venga applicato ai dati dell'oggetto.



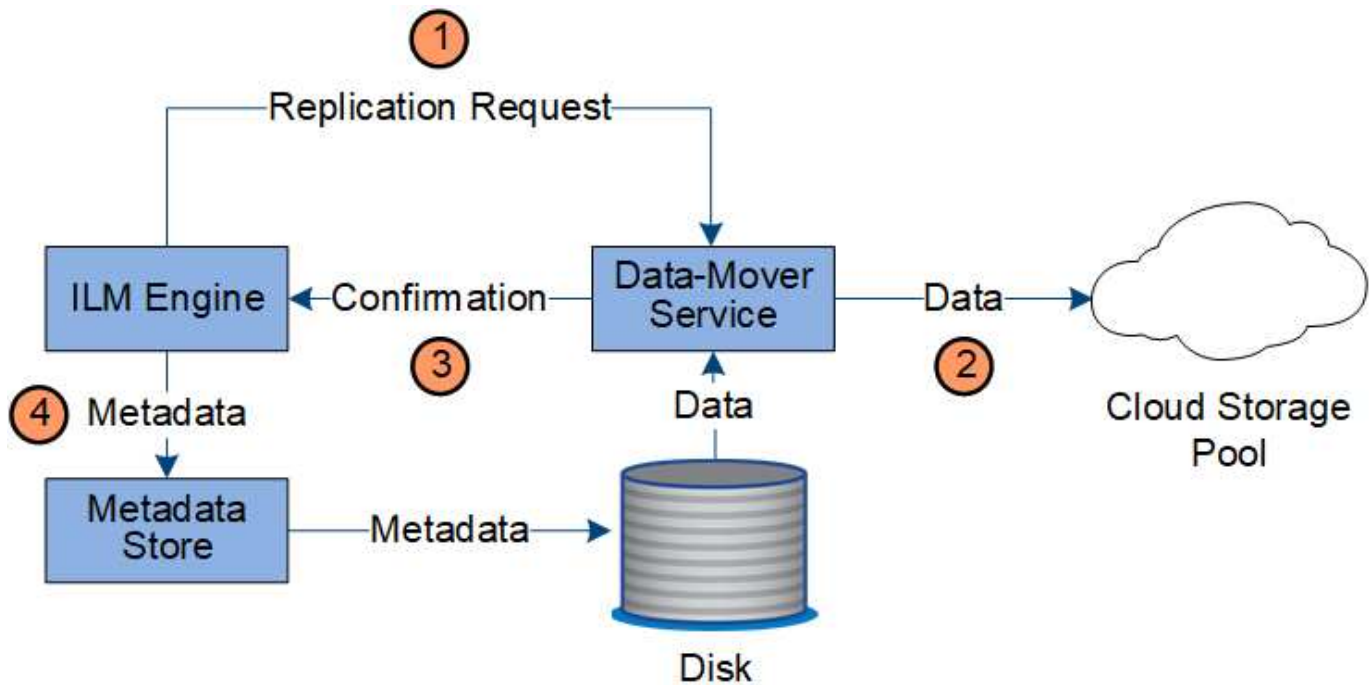
1. Il motore ILM interroga il servizio ADC per determinare quale servizio DDS può eseguire al meglio l'operazione di erasure coding. Una volta stabilito, il motore ILM invia una richiesta di "inizializzazione" a tale servizio.
2. Il servizio DDS richiede a un LDR di eseguire la cancellazione del codice dei dati dell'oggetto.
3. Il servizio LDR di origine invia una copia al servizio LDR selezionato per la cancellazione del codice.
4. Una volta suddiviso nel numero appropriato di parità e frammenti di dati, il servizio LDR distribuisce questi frammenti tra i nodi di storage (servizi Chunk) che costituiscono il pool di storage del profilo di codifica Erasure.
5. Il servizio LDR notifica al motore ILM, confermando che i dati dell'oggetto sono stati distribuiti correttamente.
6. Il motore ILM aggiorna l'archivio di metadati con i metadati della posizione dell'oggetto.

Protezione dei contenuti: Pool di storage cloud

Se le istruzioni di posizionamento del contenuto di una regola ILM richiedono che una copia replicata dei dati dell'oggetto venga memorizzata in un Cloud Storage Pool, i dati dell'oggetto vengono duplicati nel bucket S3 esterno o nel container di storage Azure Blob specificato per il Cloud Storage Pool.

Flusso di dati

Il motore ILM, che è un componente del servizio LDR, e il servizio Data Mover controllano lo spostamento degli oggetti nel Cloud Storage Pool.

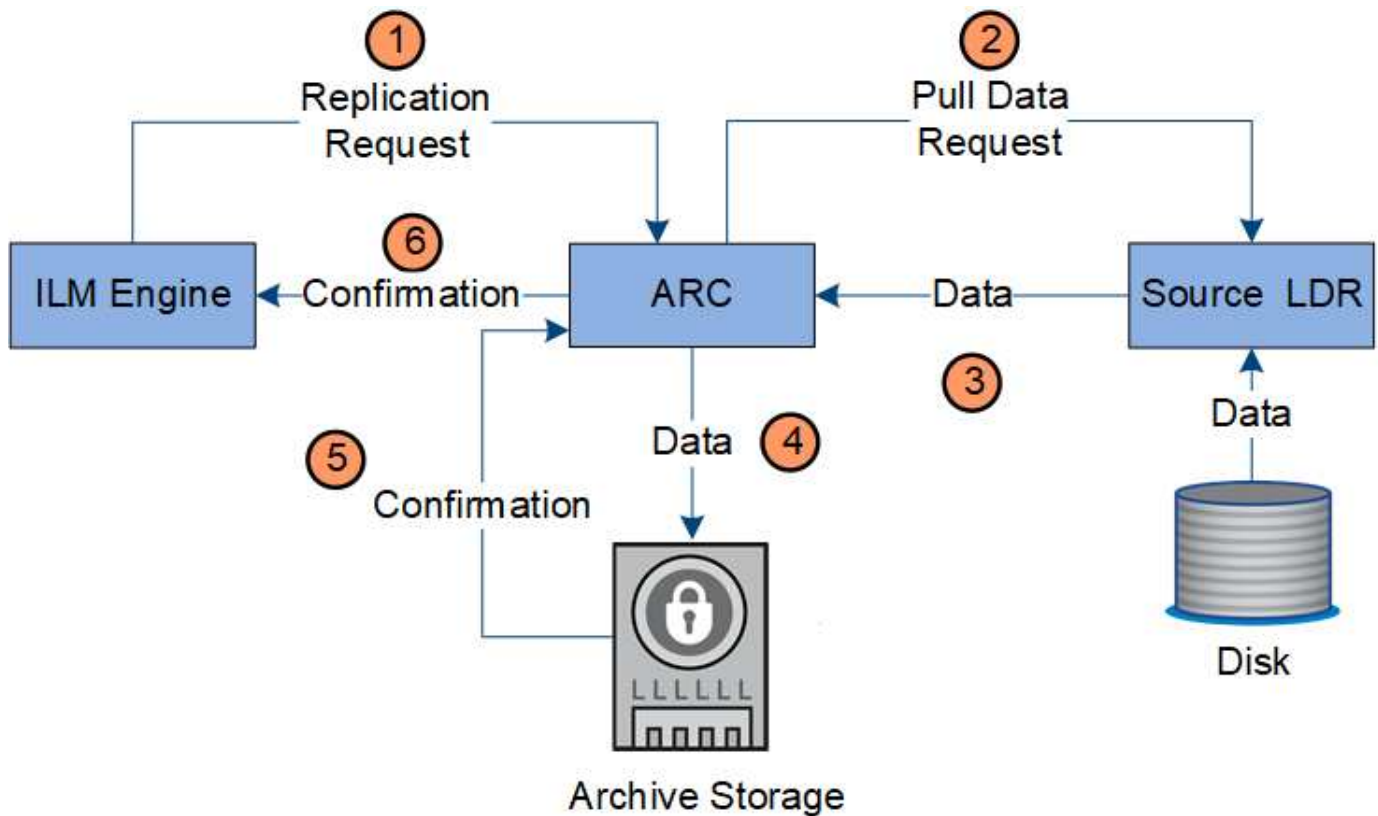


1. Il motore ILM seleziona un servizio Data Mover da replicare nel Cloud Storage Pool.
2. Il servizio Data Mover invia i dati dell'oggetto al Cloud Storage Pool.
3. Il servizio Data Mover notifica al motore ILM che i dati dell'oggetto sono stati memorizzati.
4. Il motore ILM aggiorna l'archivio di metadati con i metadati della posizione dell'oggetto.

Protezione del contenuto: Archivio

Un'operazione di archiviazione consiste in un flusso di dati definito tra il sistema StorageGRID e il client.

Se il criterio ILM richiede l'archiviazione di una copia dei dati dell'oggetto, il motore ILM, che è un componente del servizio LDR, invia una richiesta al nodo di archiviazione, che a sua volta invia una copia dei dati dell'oggetto al sistema di archiviazione di destinazione.



1. Il motore ILM invia una richiesta al servizio ARC per memorizzare una copia su un supporto di archiviazione.
2. Il servizio ARC interroga il servizio ADC per la migliore posizione di origine e invia una richiesta al servizio LDR di origine.
3. Il servizio ARC recupera i dati degli oggetti dal servizio LDR.
4. Il servizio ARC invia i dati dell'oggetto alla destinazione del supporto di archiviazione.
5. Il supporto di archiviazione notifica al servizio ARC che i dati dell'oggetto sono stati memorizzati.
6. Il servizio ARC notifica al motore ILM che i dati dell'oggetto sono stati memorizzati.

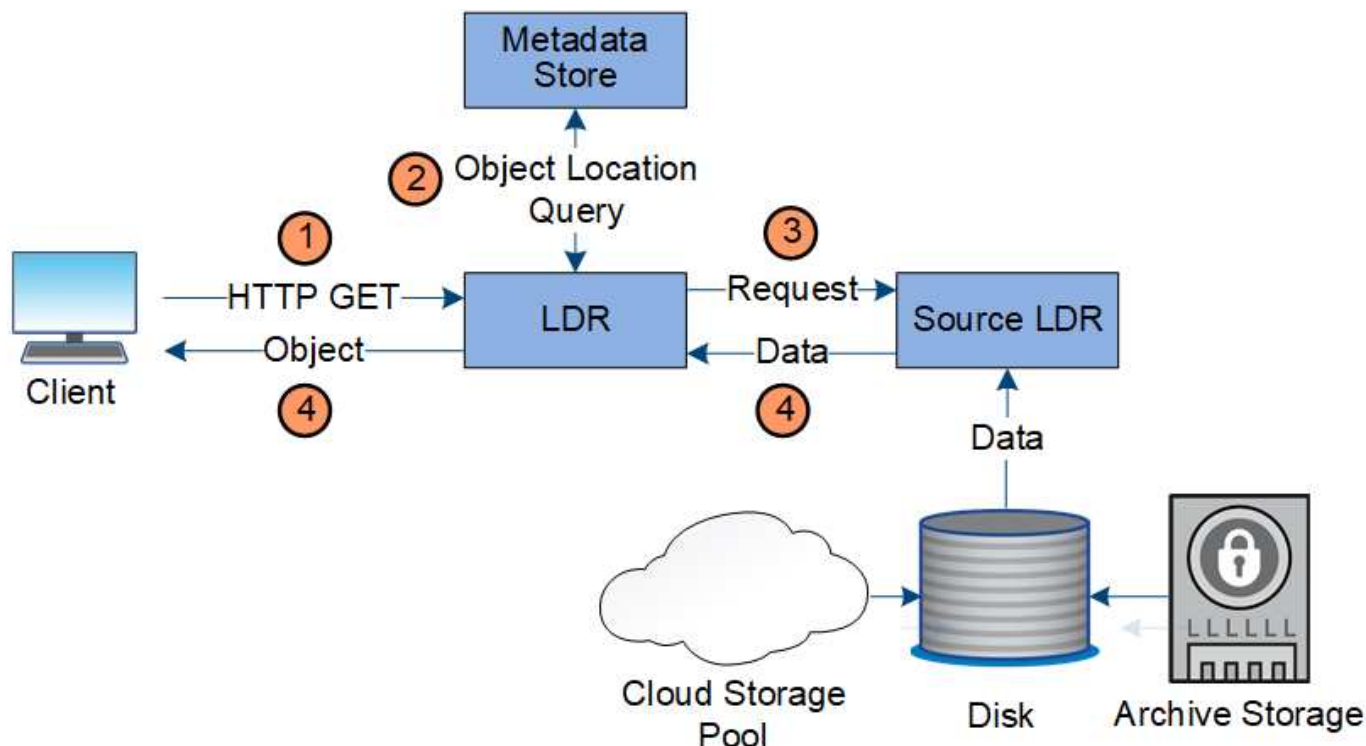
Recuperare il flusso di dati

Un'operazione di recupero consiste in un flusso di dati definito tra il sistema StorageGRID e il client. Il sistema utilizza gli attributi per tenere traccia del recupero dell'oggetto da un nodo di storage o, se necessario, da un pool di storage cloud o da un nodo di archivio.

Il servizio LDR di Storage Node interroga l'archivio di metadati per la posizione dei dati dell'oggetto e li recupera dal servizio LDR di origine. Preferenzialmente, il recupero avviene da un nodo di storage. Se l'oggetto non è disponibile su un nodo di storage, la richiesta di recupero viene indirizzata a un pool di storage cloud o a un nodo di archivio.



Se l'unica copia dell'oggetto si trova sullo storage AWS Glacier o sul Tier Azure Archive, l'applicazione client deve emettere una richiesta di ripristino S3 POST Object per ripristinare una copia recuperabile nel Cloud Storage Pool.



1. Il servizio LDR riceve una richiesta di recupero dall'applicazione client.
2. Il servizio LDR interroga l'archivio di metadati per la posizione dei dati dell'oggetto e i metadati.
3. Il servizio LDR inoltra la richiesta di recupero al servizio LDR di origine.
4. Il servizio LDR di origine restituisce i dati dell'oggetto dal servizio LDR interrogato e il sistema restituisce l'oggetto all'applicazione client.

Eliminare il flusso di dati

Tutte le copie degli oggetti vengono rimosse dal sistema StorageGRID quando un client esegue un'operazione di eliminazione o quando scade la durata dell'oggetto, attivandone la rimozione automatica. Esiste un flusso di dati definito per l'eliminazione degli oggetti.

Gerarchia di eliminazione

StorageGRID offre diversi metodi per controllare quando gli oggetti vengono conservati o cancellati. Gli oggetti possono essere cancellati automaticamente o su richiesta del client. StorageGRID assegna sempre la priorità a qualsiasi impostazione di blocco oggetti S3 rispetto alle richieste di eliminazione del client, che hanno la priorità sul ciclo di vita del bucket S3 e sulle istruzioni di posizionamento ILM.

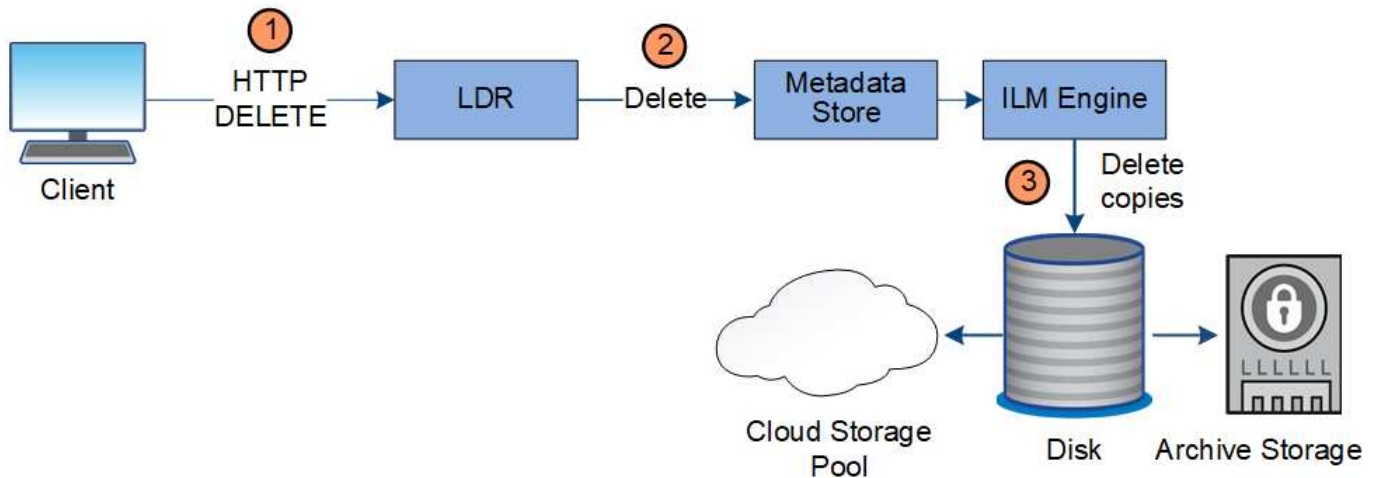
- **S3 Object Lock:** Se l'impostazione globale S3 Object Lock è attivata per la griglia, i client S3 possono creare bucket con S3 Object Lock abilitato e quindi utilizzare l'API REST S3 per specificare le impostazioni di conservazione fino alla data e conservazione legale per ogni versione di oggetto aggiunta a quel bucket.
 - Una versione dell'oggetto sottoposta a blocco legale non può essere eliminata con alcun metodo.
 - Prima che venga raggiunta la data di conservazione di una versione a oggetti, tale versione non può essere eliminata da alcun metodo.
 - Gli oggetti nei bucket con S3 Object Lock abilitato vengono conservati da ILM "forever". Tuttavia, una volta raggiunta la data di conservazione, una versione dell'oggetto può essere eliminata da una richiesta del client o dalla scadenza del ciclo di vita del bucket.

- Se i client S3 applicano una data di conservazione predefinita al bucket, non devono specificare una data di conservazione per ciascun oggetto.
- **Richiesta di eliminazione del client:** Un client S3 o Swift può emettere una richiesta di eliminazione dell'oggetto. Quando un client elimina un oggetto, tutte le copie dell'oggetto vengono rimosse dal sistema StorageGRID.
- **Ciclo di vita del bucket S3:** I client S3 possono aggiungere una configurazione del ciclo di vita ai bucket che specifica un'azione di scadenza. Se esiste un ciclo di vita del bucket, StorageGRID elimina automaticamente tutte le copie di un oggetto quando viene soddisfatta la data o il numero di giorni specificati nell'azione di scadenza, a meno che il client non elimini prima l'oggetto.
- **Istruzioni di posizionamento ILM:** Supponendo che il bucket non abbia attivato il blocco oggetti S3 e che non vi sia alcun ciclo di vita del bucket, StorageGRID elimina automaticamente un oggetto al termine dell'ultimo periodo di tempo della regola ILM e non vi sono ulteriori posizionamenti specificati per l'oggetto.



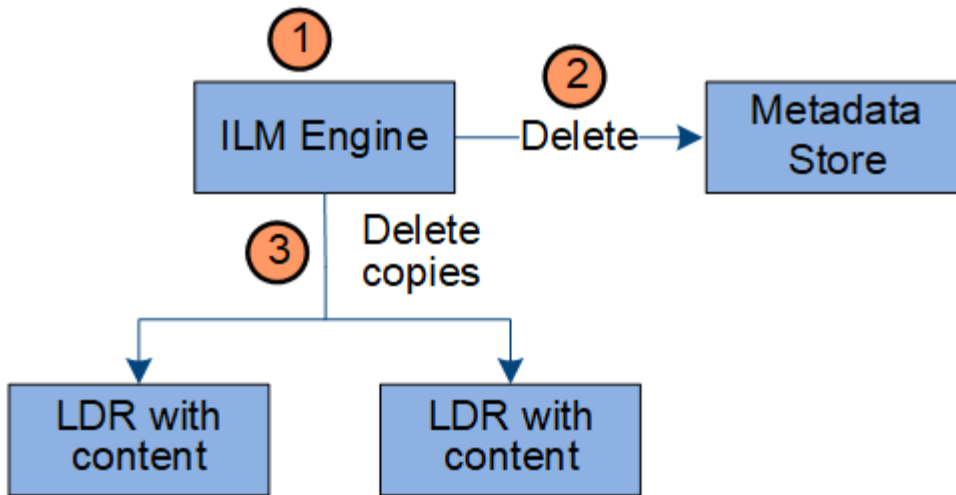
L'azione Expiration (scadenza) in un ciclo di vita del bucket S3 sovrascrive sempre le impostazioni ILM. Di conseguenza, un oggetto potrebbe essere conservato sulla griglia anche dopo che sono scadute le istruzioni ILM per il posizionamento dell'oggetto.

Eliminazione del flusso di dati per il client



1. Il servizio LDR riceve una richiesta di eliminazione dall'applicazione client.
2. Il servizio LDR aggiorna l'archivio di metadati in modo che l'oggetto venga cancellato dalle richieste del client e istruisce il motore ILM a rimuovere tutte le copie dei dati dell'oggetto.
3. L'oggetto viene rimosso dal sistema. L'archivio di metadati viene aggiornato per rimuovere i metadati degli oggetti.

Flusso di dati per l'eliminazione di ILM



1. Il motore ILM determina che l'oggetto deve essere cancellato.
2. Il motore ILM invia una notifica all'archivio di metadati. L'archivio di metadati aggiorna i metadati degli oggetti in modo che l'oggetto venga cancellato dalle richieste del client.
3. Il motore ILM rimuove tutte le copie dell'oggetto. L'archivio di metadati viene aggiornato per rimuovere i metadati degli oggetti.

Come usare StorageGRID

Esplora Grid Manager

Grid Manager è l'interfaccia grafica basata su browser che consente di configurare, gestire e monitorare il sistema StorageGRID.

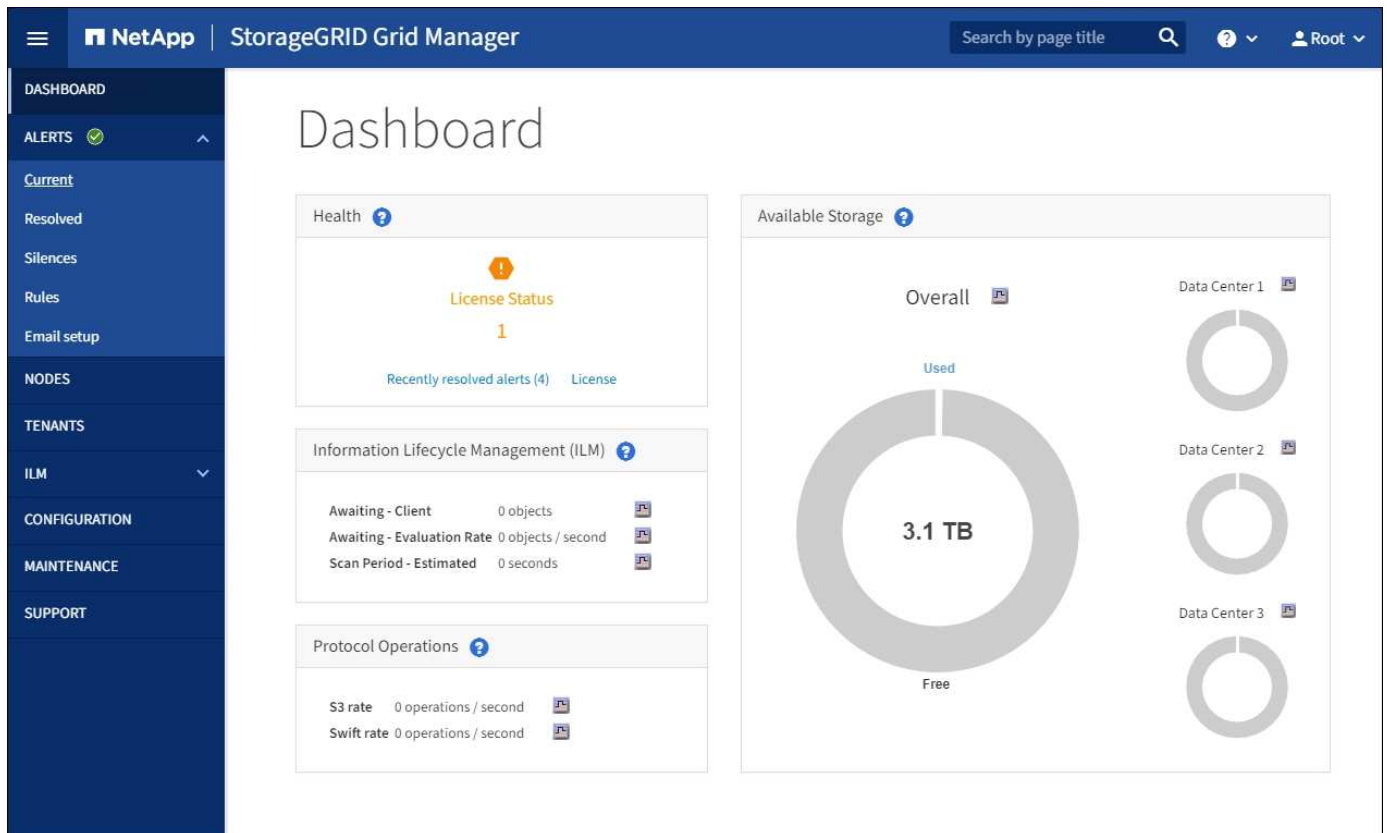
Quando si accede a Grid Manager, si sta effettuando la connessione a un nodo amministratore. Ogni sistema StorageGRID include un nodo di amministrazione primario e un numero qualsiasi di nodi di amministrazione non primari. È possibile connettersi a qualsiasi nodo amministratore e ciascun nodo amministratore visualizza una vista simile del sistema StorageGRID.


È possibile accedere a Grid Manager utilizzando un [browser web supportato](#).

Dashboard di Grid Manager

Quando accedi per la prima volta a Grid Manager, puoi utilizzare la dashboard per monitorare le attività del sistema in un colpo d'occhio.

La dashboard include informazioni riepilogative sullo stato di salute del sistema, sull'utilizzo dello storage, sui processi ILM e sulle operazioni S3 e Swift.



Per una spiegazione delle informazioni su ciascun pannello, fare clic sull'icona della guida  per quel pannello.

Scopri di più

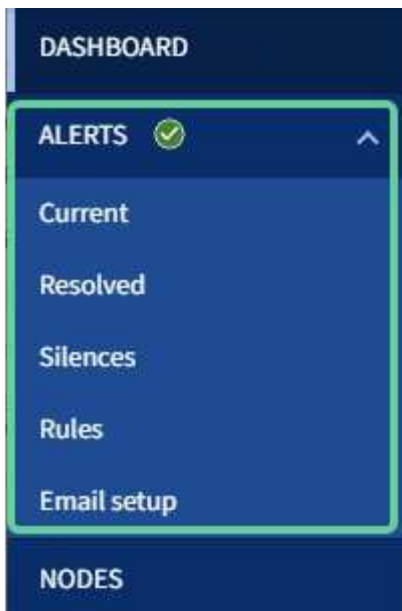
- [Monitorare e risolvere i problemi](#)

Campo di ricerca

Il campo **Search** nella barra di intestazione consente di accedere rapidamente a una pagina specifica all'interno di Grid Manager. Ad esempio, è possibile immettere **km** per accedere alla pagina Key Management Server (KMS). È possibile utilizzare **Cerca** per trovare le voci nella barra laterale di Grid Manager e nei menu Configurazione, manutenzione e supporto.

Menu Avvisi

Il menu Avvisi fornisce un'interfaccia di facile utilizzo per rilevare, valutare e risolvere i problemi che potrebbero verificarsi durante il funzionamento di StorageGRID.



Dal menu Alerts (Avvisi), è possibile effettuare le seguenti operazioni:

- Rivedere gli avvisi correnti
- Esaminare gli avvisi risolti
- Configurare i silenzi per eliminare le notifiche di avviso
- Definire le regole di avviso per le condizioni che attivano gli avvisi
- Configurare il server di posta elettronica per le notifiche degli avvisi

Scopri di più

- [Monitorare e gestire gli avvisi](#)
- [Monitorare e risolvere i problemi](#)

Pagina nodi

La pagina Nodes (nodi) visualizza informazioni sull'intera griglia, su ciascun sito della griglia e su ciascun nodo di un sito.

La home page dei nodi visualizza le metriche combinate per l'intera griglia. Per visualizzare le informazioni relative a un determinato sito o nodo, selezionare il sito o nodo.

Scopri di più

- [Gestire tenant e connessioni client](#)
- [Amministrare StorageGRID](#)
- [Utilizzare un account tenant](#)

Menu ILM

Il menu ILM consente di configurare le regole e le policy ILM (Information Lifecycle Management) che regolano la durata e la disponibilità dei dati. È inoltre possibile inserire un identificatore di oggetto per visualizzare i metadati relativi a tale oggetto.



Scopri di più

- [Utilizza la gestione del ciclo di vita delle informazioni](#)
- [Gestire gli oggetti con ILM](#)

Menu di configurazione

Il menu Configurazione consente di specificare le impostazioni di rete, di sicurezza, di sistema, di monitoraggio e di controllo degli accessi.

Configuration

Configure your StorageGRID system.

Network	Security	System	Monitoring	Access control
Domain names	Certificates	Display options	Audit and syslog server	Admin groups
High availability groups	Key management server	Grid options	SNMP agent	Admin users
Link cost	Proxy settings	S3 Object Lock		Grid passwords
Load balancer endpoints	Untrusted Client Networks	Storage options		Identity federation
Traffic classification				Single sign-on
VLAN interfaces				

Scopri di più

- [Configurare le impostazioni di rete](#)
- [Gestire tenant e connessioni client](#)
- [Esaminare i messaggi di audit](#)
- [Controllare l'accesso a StorageGRID](#)
- [Amministrare StorageGRID](#)
- [Monitorare e risolvere i problemi](#)
- [Esaminare i registri di audit](#)

Menu di manutenzione

Il menu Maintenance (manutenzione) consente di eseguire attività di manutenzione, manutenzione del sistema e manutenzione della rete.

Maintenance

Perform maintenance procedures on your StorageGRID system.

Tasks	System	Network
Decommission	License	DNS servers
Expansion	Recovery package	Grid Network
Recovery	Software update	NTP servers
Object existence check		

Attività

Le attività di manutenzione includono:

- Decommissionare le operazioni per rimuovere i nodi e i siti grid inutilizzati.
- Operazioni di espansione per aggiungere nuovi nodi e siti grid.
- Operazioni di recovery per sostituire un nodo guasto e ripristinare i dati.
- Controllo dell'esistenza di oggetti per verificare l'esistenza (anche se non la correttezza) dei dati dell'oggetto.

Sistema

Le attività di manutenzione del sistema che è possibile eseguire includono:

- Revisione dei dettagli della licenza StorageGRID corrente o caricamento di una nuova licenza.
- Generazione di un pacchetto di ripristino.
- Esecuzione di aggiornamenti software StorageGRID, inclusi aggiornamenti software, hotfix e aggiornamenti del software SANtricity OS su alcune appliance.

Rete

Le attività di manutenzione della rete che è possibile eseguire includono:

- Modifica delle informazioni sui server DNS.
- Configurazione delle subnet utilizzate nella rete Grid.
- Modifica delle informazioni sui server NTP.

Scopri di più

- [Eseguire la manutenzione](#)
- [Scaricare il pacchetto di ripristino](#)

- [Espandi il tuo grid](#)
- [Aggiornare il software](#)
- [Ripristino e manutenzione](#)
- [Appliance di storage SG6000](#)
- [Appliance di storage SG5700](#)
- [Appliance di storage SG5600](#)

Menu Support (supporto)

Il menu Support (supporto) fornisce opzioni che consentono al supporto tecnico di analizzare e risolvere i problemi del sistema. Il menu Support (supporto) comprende due parti: Tools (Strumenti) e Alarms (Allarmi) (legacy).

Support

If a problem occurs, use Support options to help technical support analyze and troubleshoot your system.

Tools	Alarms (legacy)
AutoSupport	Current alarms
Diagnostics	Historical alarms
Grid topology	Custom events
Logs	Global alarms
Metrics	Legacy email setup

Strumenti

Dalla sezione Tools (Strumenti) del menu Support (supporto), è possibile:

- Abilitare AutoSupport.
- Eseguire una serie di controlli diagnostici sullo stato corrente della griglia.
- Accedere alla struttura della topologia della griglia per visualizzare informazioni dettagliate su nodi, servizi e attributi della griglia.
- Recuperare i file di log e i dati di sistema.
- Esamina metriche e grafici dettagliati.



I tool disponibili nell'opzione **metriche** sono destinati all'utilizzo da parte del supporto tecnico. Alcune funzioni e voci di menu di questi strumenti sono intenzionalmente non funzionali.

Allarmi (legacy)

Dalla sezione Allarmi (legacy) del menu supporto, è possibile rivedere gli allarmi correnti, storici e globali, impostare eventi personalizzati e impostare notifiche e-mail per allarmi legacy e AutoSupport.



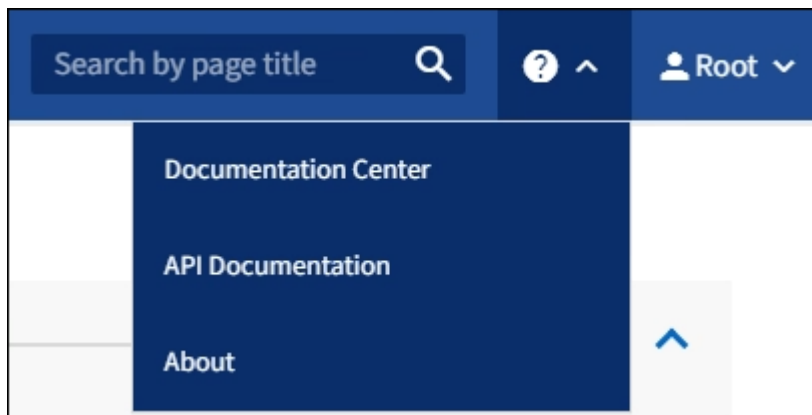
Mentre il sistema di allarme legacy continua a essere supportato, il sistema di allarme offre vantaggi significativi ed è più facile da utilizzare.

Scopri di più

- [Architettura StorageGRID e topologia di rete](#)
- [Attributi StorageGRID](#)
- [Utilizzare le opzioni di supporto di StorageGRID](#)
- [Amministrare StorageGRID](#)
- [Monitorare e risolvere i problemi](#)

Menu Guida

L'opzione Guida consente di accedere al Centro documentazione StorageGRID per la release corrente e alla documentazione API. È inoltre possibile determinare quale versione di StorageGRID è attualmente installata.



Scopri di più

- [Amministrare StorageGRID](#)

Esplora il tenant manager

Tenant Manager è l'interfaccia grafica basata su browser a cui gli utenti tenant accedono per configurare, gestire e monitorare i propri account di storage.

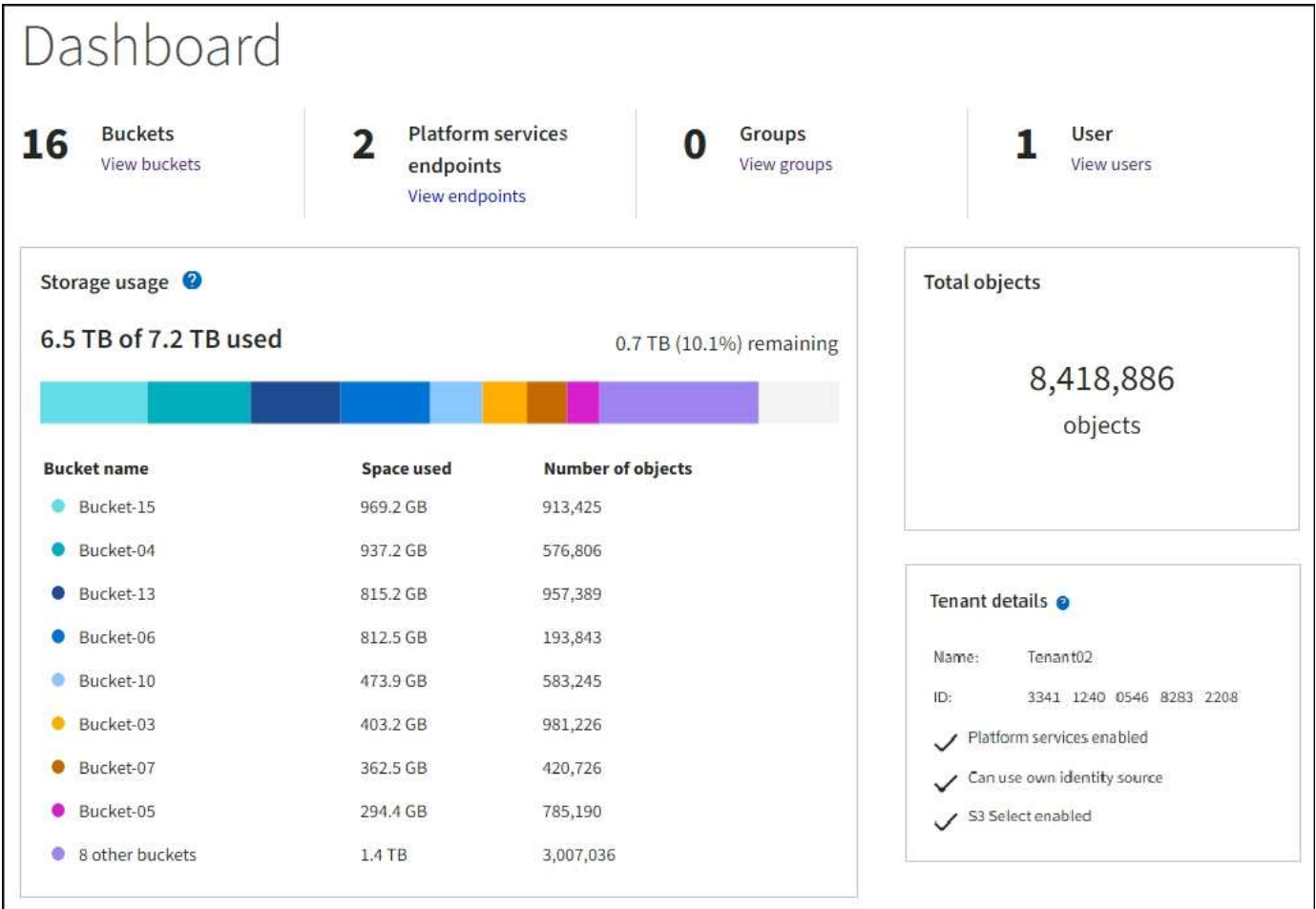
Quando gli utenti tenant accedono a Tenant Manager, si connettono a un nodo Admin.

Dashboard di tenant Manager

Dopo che un amministratore di grid ha creato un account tenant utilizzando Grid Manager o l'API Grid Management, gli utenti del tenant possono accedere a Tenant Manager.

La dashboard di Tenant Manager consente agli utenti del tenant di monitorare l'utilizzo dello storage in un colpo d'occhio. Il pannello Storage Use (utilizzo storage) contiene un elenco dei bucket più grandi (S3) o container (Swift) per il tenant. Il valore spazio utilizzato è la quantità totale di dati oggetto nel bucket o nel container. Il grafico a barre rappresenta le dimensioni relative di questi bucket o container.

Il valore visualizzato sopra il grafico a barre è la somma dello spazio utilizzato per tutti i bucket o i container del tenant. Se al momento della creazione dell’account è stato specificato il numero massimo di gigabyte, terabyte o petabyte disponibili per il tenant, viene visualizzata anche la quantità di quota utilizzata e rimanente.



Menu Storage (solo tenant S3)

Il menu Storage (archiviazione) è disponibile solo per gli account tenant S3. Questo menu consente agli utenti S3 di gestire le chiavi di accesso, creare ed eliminare bucket e gestire gli endpoint del servizio della piattaforma.



Chiavi di accesso personali

Gli utenti del tenant S3 possono gestire le chiavi di accesso come segue:

- Gli utenti che dispongono dell'autorizzazione Gestisci credenziali S3 possono creare o rimuovere le proprie chiavi di accesso S3.
- Gli utenti che dispongono dell'autorizzazione Root Access possono gestire le chiavi di accesso per l'account root S3, il proprio account e tutti gli altri utenti. Le chiavi di accesso root forniscono anche l'accesso completo ai bucket e agli oggetti del tenant, a meno che non vengano disabilitate esplicitamente da una policy del bucket.



La gestione delle chiavi di accesso per altri utenti avviene dal menu Gestione accessi.

Bucket

Gli utenti del tenant S3 con le autorizzazioni appropriate possono eseguire le seguenti attività relative ai bucket:

- Creare bucket
- Attiva blocco oggetti S3 per un nuovo bucket (presuppone che il blocco oggetti S3 sia abilitato per il sistema StorageGRID)
- Aggiornare le impostazioni del livello di coerenza
- Applicare un'impostazione di conservazione predefinita
- Configurare la condivisione delle risorse tra origini (CORS)
- Attiva e disattiva le impostazioni dell'ultimo aggiornamento dell'ora di accesso per i bucket appartenenti al tenant
- Eliminare i bucket vuoti
- Gestire gli oggetti in un bucket utilizzando [Console S3 sperimentale](#)

Se un amministratore di grid ha abilitato l'utilizzo dei servizi della piattaforma per l'account tenant, un utente tenant S3 con le autorizzazioni appropriate può eseguire anche queste attività:

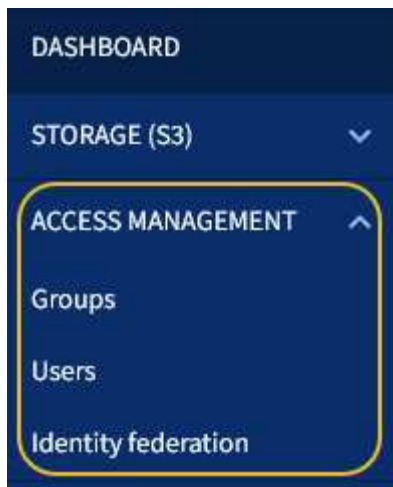
- Configurare le notifiche degli eventi S3, che possono essere inviate a un servizio di destinazione che supporta AWS Simple Notification Service™ (SNS).
- Configurare la replica di CloudMirror, che consente al tenant di replicare automaticamente gli oggetti in un bucket S3 esterno.
- Configurare l'integrazione della ricerca, che invia i metadati degli oggetti a un indice di ricerca di destinazione ogni volta che un oggetto viene creato, cancellato o i relativi metadati o tag vengono aggiornati.

Endpoint dei servizi di piattaforma

Se un amministratore di grid ha abilitato l'utilizzo dei servizi di piattaforma per l'account tenant, un utente tenant S3 con l'autorizzazione Gestisci endpoint può configurare un endpoint di destinazione per ciascun servizio di piattaforma.

Accedere al menu Gestione

Il menu Gestione accessi consente ai tenant StorageGRID di importare gruppi di utenti da un'origine di identità federata e assegnare autorizzazioni di gestione. I tenant possono anche gestire utenti e gruppi di tenant locali, a meno che il single sign-on (SSO) non sia attivo per l'intero sistema StorageGRID.



Informazioni correlate

- [Esplora Grid Manager](#)
- [Utilizzare un account tenant](#)

Controllare l'accesso a StorageGRID

È possibile controllare chi può accedere a StorageGRID e quali attività possono essere eseguite dagli utenti creando o importando gruppi e utenti e assegnando autorizzazioni a ciascun gruppo. Facoltativamente, è possibile attivare SSO (Single Sign-on), creare certificati client e modificare le password della griglia.

Controlla l'accesso a Grid Manager

È possibile determinare chi può accedere a Grid Manager e all'API Grid Management importando gruppi e utenti da un servizio di federazione delle identità o impostando gruppi locali e utenti locali.

L'utilizzo della federazione delle identità rende più rapida la configurazione di gruppi e utenti e consente agli utenti di accedere a StorageGRID utilizzando credenziali familiari. È possibile configurare la federazione delle identità se si utilizza Active Directory, OpenLDAP o Oracle Directory Server.



Se si desidera utilizzare un altro servizio LDAP v3, contattare il supporto tecnico.

È possibile determinare le attività che ciascun utente può eseguire assegnando autorizzazioni diverse a ciascun gruppo. Ad esempio, è possibile che gli utenti di un gruppo siano in grado di gestire le regole ILM e che gli utenti di un altro gruppo eseguano le attività di manutenzione. Per accedere al sistema, un utente deve appartenere ad almeno un gruppo.

Facoltativamente, è possibile configurare un gruppo in modo che sia di sola lettura. Gli utenti di un gruppo di sola lettura possono visualizzare solo le impostazioni e le funzionalità. Non possono apportare modifiche o eseguire operazioni nell'API Grid Manager o Grid Management.

Attiva single sign-on

Il sistema StorageGRID supporta SSO (Single Sign-on) 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.

Quando SSO è attivato e gli utenti accedono a StorageGRID, vengono reindirizzati alla pagina SSO dell'organizzazione per convalidare le proprie credenziali. Quando gli utenti si disconnettono da un nodo di amministrazione, vengono automaticamente disconnessi da tutti i nodi di amministrazione.

Modificare le password della griglia

La passphrase di provisioning è necessaria per molte procedure di installazione e manutenzione e per scaricare il pacchetto di ripristino StorageGRID. La passphrase è necessaria anche per scaricare i backup delle informazioni sulla topologia della griglia e delle chiavi di crittografia per il sistema StorageGRID. È possibile modificare questa passphrase in base alle esigenze.

Informazioni correlate

- [Amministrare StorageGRID](#)
- [Utilizzare un account tenant](#)

Gestire tenant e connessioni client

In qualità di amministratore di grid, è possibile creare e gestire gli account tenant utilizzati dai client S3 e Swift per memorizzare e recuperare gli oggetti e gestire le opzioni di configurazione che controllano il modo in cui i client si connettono al sistema StorageGRID.

Account tenant

Un account tenant consente di specificare chi può utilizzare il sistema StorageGRID per memorizzare e recuperare gli oggetti e quali funzionalità sono disponibili. Gli account tenant consentono alle applicazioni client che supportano l'API REST S3 o l'API REST Swift di memorizzare e recuperare oggetti su StorageGRID. Ogni account tenant utilizza il protocollo client S3 o il protocollo client Swift.

È necessario creare almeno un account tenant per ogni protocollo client che verrà utilizzato per memorizzare gli oggetti nel sistema StorageGRID. Se si desidera separare gli oggetti memorizzati nel sistema da diverse entità, è possibile creare ulteriori account tenant. Ogni account tenant dispone di gruppi e utenti federati o locali e di bucket (container per Swift) e oggetti propri.

È possibile utilizzare Grid Manager o l'API Grid Management per creare account tenant. Quando si crea un account tenant, si specificano le seguenti informazioni:

- Nome visualizzato per il tenant (l'ID account del tenant viene assegnato automaticamente e non può essere modificato).
- Se l'account tenant utilizzerà S3 o Swift.
- Per gli account tenant S3: Se l'account tenant è autorizzato a utilizzare i servizi della piattaforma. Se è consentito l'utilizzo dei servizi della piattaforma, la griglia deve essere configurata per supportarne l'utilizzo.
- Facoltativamente, una quota di storage per l'account tenant, ovvero il numero massimo di gigabyte, terabyte o petabyte disponibili per gli oggetti del tenant. La quota di storage di un tenant rappresenta una quantità logica (dimensione dell'oggetto), non una quantità fisica (dimensione sul disco).
- Se la federazione delle identità è attivata per il sistema StorageGRID, il gruppo federato dispone dell'autorizzazione di accesso root per configurare l'account tenant.
- Se l'SSO (Single Sign-on) non è in uso per il sistema StorageGRID, se l'account tenant utilizzerà la propria origine di identità o condividerà l'origine di identità della griglia e la password iniziale per l'utente root locale del tenant.

Se gli account tenant S3 devono soddisfare i requisiti normativi, gli amministratori della griglia possono attivare l'impostazione globale S3 Object Lock per il sistema StorageGRID. Quando S3 Object Lock è attivato per il sistema, tutti gli account tenant S3 possono creare bucket con S3 Object Lock attivato e specificare le impostazioni di conservazione e conservazione legale per le versioni degli oggetti in quel bucket.

Una volta creato un account tenant, gli utenti tenant possono accedere al tenant manager.

Connessioni client ai nodi StorageGRID

Prima che gli utenti tenant possano utilizzare i client S3 o Swift per memorizzare e recuperare i dati in StorageGRID, è necessario decidere come questi client si conatteranno ai nodi StorageGRID.

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

- Il servizio Load Balancer sui nodi Admin o Gateway. Questa è la connessione consigliata.
- Il servizio CLB sui nodi gateway.



Il servizio CLB è obsoleto.

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

Quando si configura StorageGRID in modo che i client possano utilizzare il servizio bilanciamento del carico, attenersi alla seguente procedura:

1. Configurare facoltativamente i gruppi ad alta disponibilità (ha). Se si crea un gruppo ha, le interfacce di più nodi Admin e nodi Gateway vengono inserite in una configurazione di backup attivo. Le connessioni client vengono effettuate utilizzando l'indirizzo IP virtuale del gruppo ha.
2. Configurare gli endpoint per il servizio Load Balancer. Il servizio Load Balancer sui nodi di amministrazione o gateway distribuisce le connessioni di rete in entrata dalle applicazioni client ai nodi di storage. Quando si crea un endpoint di bilanciamento del carico, specificare un numero di porta, se l'endpoint accetta connessioni HTTP o HTTPS, il tipo di client (S3 o Swift) che utilizzerà l'endpoint e il certificato da utilizzare per le connessioni HTTPS (se applicabile).
3. Facoltativamente, specificare che la rete client di un nodo non è attendibile per garantire che tutte le connessioni alla rete client del nodo si verifichino sugli endpoint del bilanciamento del carico.

Informazioni correlate

- [Amministrare StorageGRID](#)
- [Utilizzare un account tenant](#)
- [Utilizzare S3](#)
- [USA Swift](#)
- [Esplora il tenant manager](#)
- [Configurare le impostazioni di rete](#)

Configurare le impostazioni di rete

È possibile configurare diverse impostazioni di rete da Gestione griglia per ottimizzare il funzionamento del sistema StorageGRID.

Nomi di dominio

Se si prevede di supportare le richieste in stile host virtuale S3, è necessario configurare l'elenco dei nomi di dominio degli endpoint a cui si connettono i client S3. Alcuni esempi sono `s3.example.com`, `s3.example.co.uk`, e `s3-east.example.com`.

I certificati del server configurati devono corrispondere ai nomi di dominio degli endpoint.

Gruppi ad alta disponibilità

È possibile utilizzare i gruppi ad alta disponibilità (ha) per fornire connessioni dati altamente disponibili per i client S3 e Swift o per fornire connessioni altamente disponibili a Grid Manager e Tenant Manager.

Quando si crea un gruppo ha, si seleziona un'interfaccia di rete per uno o più nodi. Ciascun gruppo ha fornisce l'accesso ai servizi condivisi sui nodi selezionati.

- I gruppi HA che includono interfacce su nodi gateway, nodi di amministrazione o entrambi forniscono connessioni dati altamente disponibili per i client S3 e Swift.
- I gruppi HA che includono interfacce sui nodi di amministrazione forniscono solo connessioni altamente disponibili al Grid Manager e al Tenant Manager.

Le interfacce possono appartenere a Grid Network (eth0), Client Network (eth2) o a una rete VLAN.

È possibile assegnare fino a 10 indirizzi IP virtuali (VIP) a ciascun gruppo ha. Specificare un'interfaccia come principale e classificare le altre interfacce in ordine di priorità. L'interfaccia principale è l'interfaccia attiva a meno che non si verifichi un errore. Se l'interfaccia attiva non riesce, gli indirizzi VIP passano alla prima interfaccia di backup nell'ordine di priorità. Se l'interfaccia non funziona, gli indirizzi VIP passano all'interfaccia di backup successiva e così via.

Costi di collegamento

È possibile regolare i costi dei collegamenti in modo da riflettere la latenza tra i siti. Quando esistono due o più siti del data center, i costi di collegamento danno la priorità a quale sito del data center deve fornire un servizio richiesto.

Endpoint del bilanciamento del carico

È possibile utilizzare un bilanciamento del carico per gestire i carichi di lavoro di acquisizione e recupero dai client S3 e Swift. Il bilanciamento del carico massimizza la velocità e la capacità di connessione distribuendo i carichi di lavoro e le connessioni tra più nodi di storage.

Se si desidera utilizzare il servizio di bilanciamento del carico di StorageGRID, incluso nei nodi di amministrazione e nei nodi gateway, è necessario configurare uno o più endpoint di bilanciamento del carico. Ogni endpoint definisce una porta Gateway Node o Admin Node per le richieste S3 e Swift ai nodi di storage.

Classificazione del traffico

È possibile creare policy di classificazione del traffico per identificare e gestire diversi tipi di traffico di rete, incluso il traffico relativo a bucket, tenant, subnet client o endpoint del bilanciamento del carico specifici. Queste policy possono essere utili per la limitazione e il monitoraggio del traffico.

Interfacce VLAN

È possibile creare interfacce LAN virtuali (VLAN) per isolare e partizionare il traffico per garantire sicurezza, flessibilità e performance. Ogni interfaccia VLAN è associata a una o più interfacce principali sui nodi Admin e

Gateway. È possibile utilizzare le interfacce VLAN nei gruppi ha e negli endpoint del bilanciamento del carico per separare il traffico client o amministrativo in base all'applicazione o al tenant.

Ad esempio, la rete potrebbe utilizzare la VLAN 100 per il traffico FabricPool e la VLAN 200 per un'applicazione di archiviazione.

Informazioni correlate

- [Amministrare StorageGRID](#)
- [Gestire tenant e connessioni client](#)

Configurare le impostazioni di sicurezza

È possibile configurare diverse impostazioni di sicurezza da Gestione griglia per proteggere il sistema StorageGRID.

Certificati

StorageGRID utilizza due tipi di certificati di sicurezza:

- I certificati del server sono richiesti quando si utilizzano connessioni HTTPS. I certificati del server vengono utilizzati per stabilire connessioni sicure tra client e server, autenticando l'identità di un server nei suoi client e fornendo un percorso di comunicazione sicuro per i dati. Il server e il client dispongono di una copia del certificato.
- I certificati client autenticano un'identità del client o dell'utente nel server, fornendo un'autenticazione più sicura rispetto alle sole password. I certificati client non crittografano i dati.

È possibile visualizzare tutti i certificati StorageGRID nella pagina **CONFIGURAZIONE sicurezza certificati**.

Server di gestione delle chiavi

È possibile configurare uno o più server di gestione delle chiavi esterni (KMS) per fornire chiavi di crittografia ai servizi StorageGRID e alle appliance di storage. Ogni cluster KMS o KMS utilizza il protocollo KMIP (Key Management Interoperability Protocol) per fornire una chiave di crittografia ai nodi appliance nel sito StorageGRID associato. L'utilizzo di server di gestione delle chiavi consente di proteggere i dati StorageGRID anche se un'appliance viene rimossa dal data center. Una volta crittografati i volumi dell'appliance, non è possibile accedere ai dati dell'appliance a meno che il nodo non sia in grado di comunicare con il KMS.



Per utilizzare la gestione delle chiavi di crittografia, è necessario attivare l'impostazione **Node Encryption** per ogni appliance durante l'installazione, prima di aggiungere l'appliance alla griglia.

Impostazioni del proxy

Se si utilizzano i servizi della piattaforma S3 o i Cloud Storage Pools, è possibile configurare un server proxy non trasparente tra i nodi di storage e gli endpoint S3 esterni. Se si inviano messaggi AutoSupport utilizzando HTTPS o HTTP, è possibile configurare un server proxy non trasparente tra i nodi di amministrazione e il supporto tecnico.

Proxy Settings
Storage
Admin

Reti client non attendibili

Se si utilizza una rete client, è possibile proteggere StorageGRID da attacchi ostili specificando che la rete client di ciascun nodo non è attendibile. Se la rete client di un nodo non è attendibile, il nodo accetta solo connessioni in entrata su porte esplicitamente configurate come endpoint del bilanciamento del carico.

Ad esempio, è possibile che un nodo gateway rifiuti tutto il traffico in entrata sulla rete client ad eccezione delle richieste HTTPS S3. In alternativa, è possibile attivare il traffico del servizio della piattaforma S3 in uscita da un nodo di storage, impedendo al contempo eventuali connessioni in entrata a tale nodo di storage sulla rete client.

Informazioni correlate

- [Amministrare StorageGRID](#)
- [Gestire tenant e connessioni client](#)

Configurare le impostazioni di sistema

È possibile configurare diverse impostazioni di sistema da Gestione griglia per ottimizzare il funzionamento del sistema StorageGRID.

Opzioni di visualizzazione

Le opzioni di visualizzazione consentono di specificare il periodo di timeout per le sessioni utente e di eliminare le notifiche e-mail per gli allarmi legacy e i messaggi AutoSupport attivati dagli eventi.

Opzioni della griglia

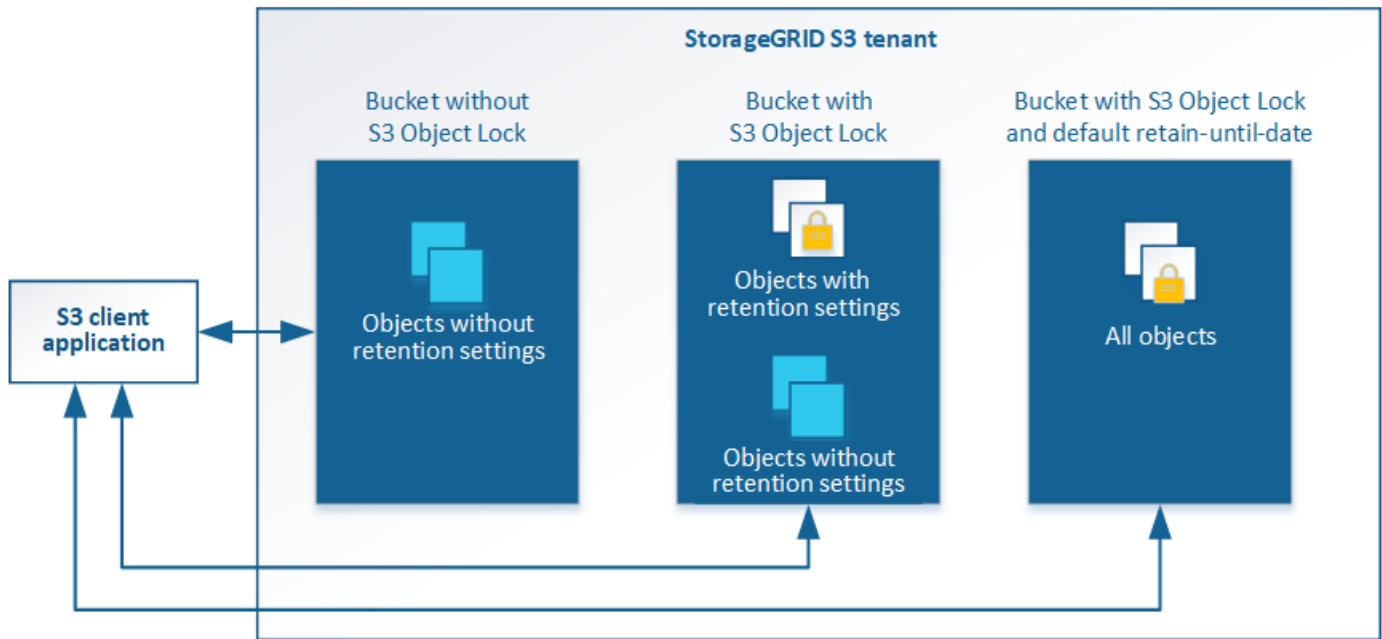
È possibile utilizzare Opzioni griglia per configurare le impostazioni per tutti gli oggetti memorizzati nel sistema StorageGRID, inclusa la compressione degli oggetti memorizzati e la crittografia degli oggetti memorizzati. e l'hashing degli oggetti memorizzati.

È inoltre possibile utilizzare queste opzioni per specificare le impostazioni globali per le operazioni dei client S3 e Swift.

Blocco oggetti S3

La funzione blocco oggetti StorageGRID S3 è una soluzione di protezione degli oggetti equivalente a blocco oggetti S3 in Amazon Simple Storage Service (Amazon S3). È possibile attivare l'impostazione di blocco oggetti S3 globale per un sistema StorageGRID per consentire agli account tenant S3 di creare bucket con blocco oggetti S3 attivato. Il tenant può quindi utilizzare un'applicazione client S3 per specificare facoltativamente le impostazioni di conservazione (conserva fino alla data, conservazione legale o entrambe) per gli oggetti in tali bucket. Inoltre, ogni bucket con S3 Object Lock abilitato può disporre di una modalità di conservazione e di un periodo di conservazione predefiniti, che si applicano se gli oggetti vengono aggiunti al bucket senza le proprie impostazioni di conservazione.

StorageGRID with S3 Object Lock setting enabled



Opzioni di storage

Le opzioni di storage consentono di controllare la segmentazione degli oggetti e di ignorare le impostazioni di filigrana del volume di storage per gestire lo spazio di storage utilizzabile di un nodo di storage.

Utilizza la gestione del ciclo di vita delle informazioni

Si utilizza la gestione del ciclo di vita delle informazioni (ILM) per controllare il posizionamento, la durata e la protezione dei dati per tutti gli oggetti nel sistema StorageGRID. Le regole ILM determinano il modo in cui StorageGRID memorizza gli oggetti nel tempo. Configurare una o più regole ILM e aggiungerle a un criterio ILM.

Le regole ILM definiscono:

- Quali oggetti devono essere memorizzati. Una regola può essere applicata a tutti gli oggetti oppure è possibile specificare filtri per identificare gli oggetti a cui si applica una regola. Ad esempio, una regola può essere applicata solo agli oggetti associati a determinati account tenant, a specifici bucket S3 o a contenitori Swift o a specifici valori di metadati.
- Il tipo e la posizione di storage. Gli oggetti possono essere memorizzati nei nodi di storage, nei pool di storage cloud o nei nodi di archiviazione.
- Il tipo di copie a oggetti eseguite. Le copie possono essere replicate o codificate per la cancellazione.
- Per le copie replicate, il numero di copie eseguite.
- Per le copie codificate erasure, viene utilizzato lo schema di erasure coding.
- Il cambia nel tempo nella posizione di storage di un oggetto e nel tipo di copie.
- Modalità di protezione dei dati degli oggetti durante l'acquisizione degli oggetti nella griglia (posizionamento sincrono o doppio commit).

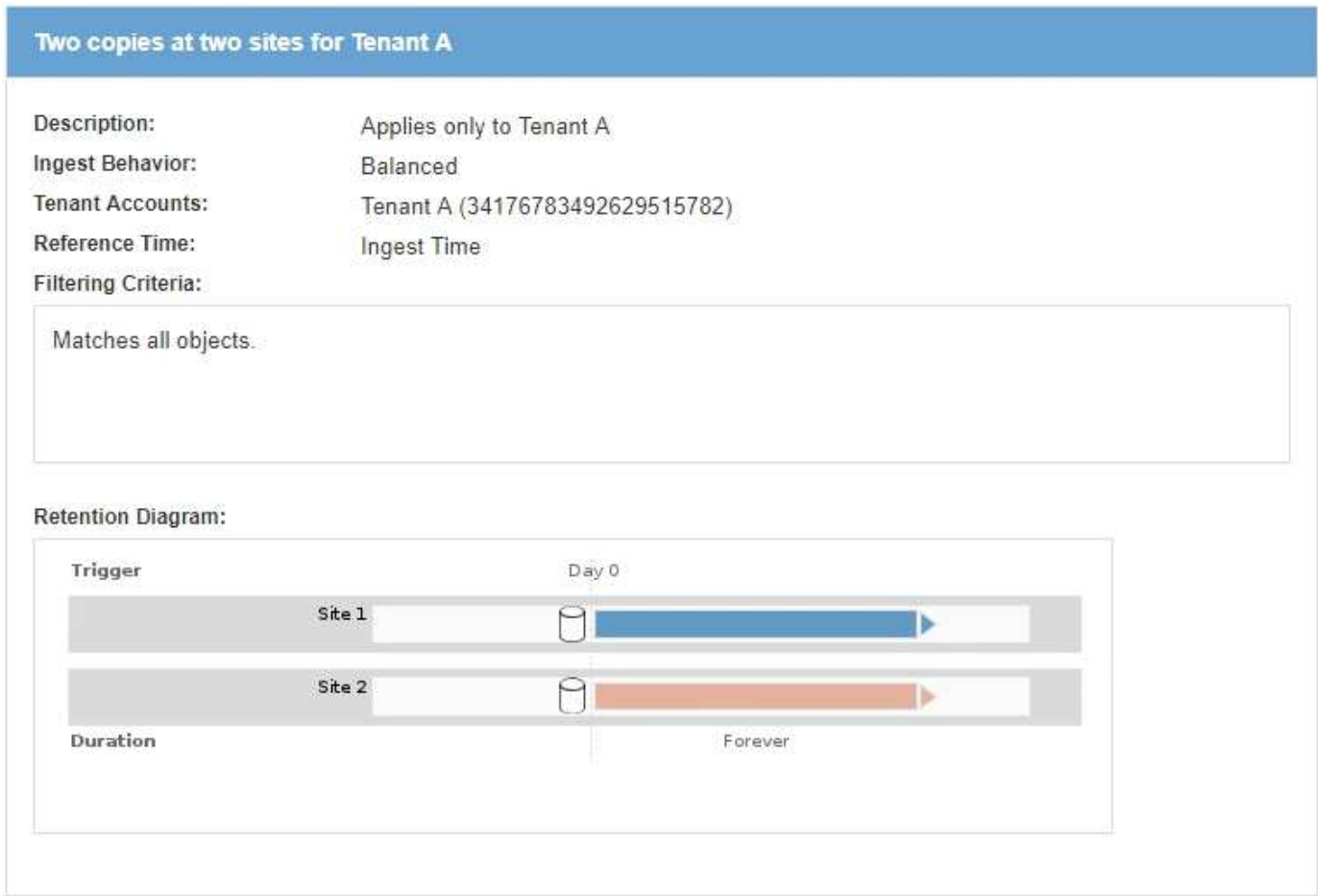
Si noti che i metadati degli oggetti non sono gestiti dalle regole ILM. I metadati degli oggetti vengono invece memorizzati in un database Cassandra in un archivio di metadati. Tre copie dei metadati degli oggetti vengono gestite automaticamente in ogni sito per proteggere i dati dalla perdita. Le copie sono distribuite

uniformemente in tutti i nodi di storage.

Esempio di regola ILM

Questo esempio di regola ILM si applica agli oggetti appartenenti al tenant A. Esegue due copie replicate di tali oggetti e memorizza ciascuna copia in un sito diverso. Le due copie vengono conservate “forever,” il che significa che StorageGRID non le eliminerà automaticamente. Al contrario, StorageGRID conserverà questi oggetti fino a quando non saranno cancellati da una richiesta di eliminazione del client o dalla scadenza di un ciclo di vita del bucket.

Questa regola utilizza l’opzione bilanciata per il comportamento di acquisizione: L’istruzione di posizionamento a due siti viene applicata non appena il tenant A salva un oggetto in StorageGRID, a meno che non sia possibile eseguire immediatamente entrambe le copie richieste. Ad esempio, se il sito 2 non è raggiungibile quando il tenant A salva un oggetto, StorageGRID eseguirà due copie intermedie sui nodi di storage nel sito 1. Non appena il sito 2 sarà disponibile, StorageGRID effettuerà la copia richiesta presso il sito.



Come un criterio ILM valuta gli oggetti

Il criterio ILM attivo per il sistema StorageGRID controlla il posizionamento, la durata e la protezione dei dati di tutti gli oggetti.

Quando i client salvano gli oggetti in StorageGRID, gli oggetti vengono valutati in base all’insieme ordinato di regole ILM nel criterio attivo, come segue:

1. Se i filtri per la prima regola del criterio corrispondono a un oggetto, l’oggetto viene acquisito in base al comportamento di acquisizione di tale regola e memorizzato in base alle istruzioni di posizionamento di tale regola.

2. Se i filtri per la prima regola non corrispondono all'oggetto, l'oggetto viene valutato in base a ogni regola successiva nel criterio fino a quando non viene effettuata una corrispondenza.
3. Se nessuna regola corrisponde a un oggetto, vengono applicate le istruzioni di inserimento e posizionamento della regola predefinita nel criterio. La regola predefinita è l'ultima regola di un criterio e non può utilizzare alcun filtro. Deve essere applicato a tutti i tenant, a tutti i bucket e a tutte le versioni degli oggetti.

Esempio di policy ILM

Questo esempio di policy ILM utilizza tre regole ILM.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name

Reason for change

Rules

1. Select the rules you want to add to the policy.
2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

+ Select Rules

	Default	Rule Name	Tenant Account	Actions
⊕		Rule 1: 3 replicated copies for Tenant A	Tenant A (58889986524346589742)	✕
⊕		Rule 2: Erasure coding for objects greater than 1 MB	—	✕
	✓	Rule 3: 2 copies 2 data centers (default)	—	✕

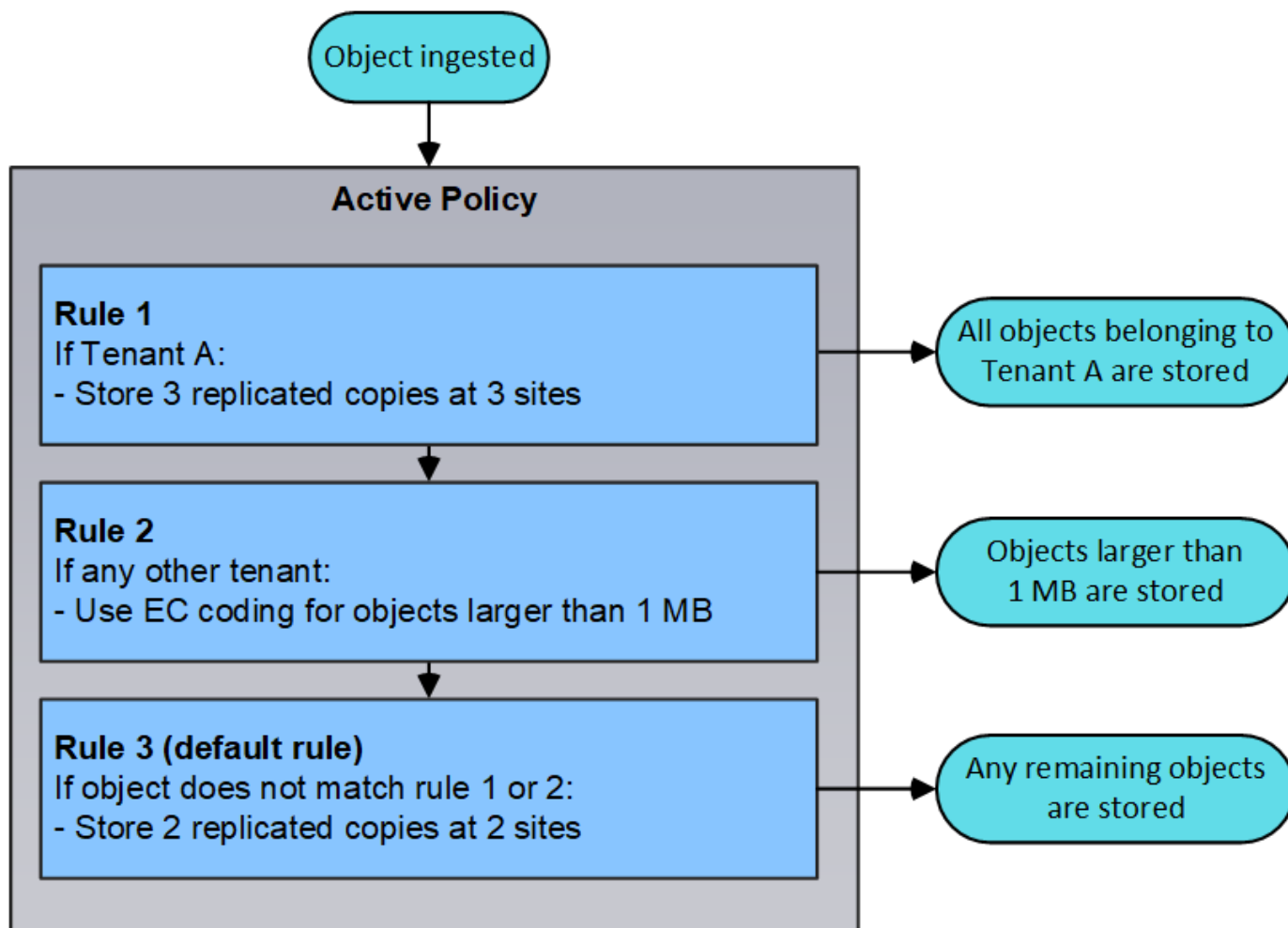
Cancel

Save

In questo esempio, la regola 1 corrisponde a tutti gli oggetti appartenenti al tenant A. Questi oggetti vengono memorizzati come tre copie replicate in tre siti. Gli oggetti appartenenti ad altri tenant non corrispondono alla regola 1, quindi vengono valutati in base alla regola 2.

La regola 2 corrisponde a tutti gli oggetti degli altri tenant, ma solo se sono superiori a 1 MB. Questi oggetti più grandi vengono memorizzati utilizzando la codifica di cancellazione 6+3 in tre siti. La regola 2 non corrisponde a oggetti di dimensioni pari o inferiori a 1 MB, pertanto questi oggetti vengono valutati in base alla regola 3.

La regola 3 è l'ultima regola predefinita del criterio e non utilizza filtri. La regola 3 crea due copie replicate di tutti gli oggetti non corrispondenti alla regola 1 o alla regola 2 (oggetti non appartenenti al tenant A di dimensioni pari o inferiori a 1 MB).



Informazioni correlate

- [Gestire gli oggetti con ILM](#)

Monitorare le operazioni


Visualizzare la pagina nodi

Quando hai bisogno di informazioni più dettagliate sul tuo sistema StorageGRID rispetto a quelle fornite dalla dashboard, puoi utilizzare la pagina Nodes per visualizzare le metriche per l'intera griglia, ogni sito nella griglia e ogni nodo di un sito.

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Webscale Deployment	Grid	0%	0%	—
DC1	Site	0%	0%	—
DC1-ADM1	Primary Admin Node	—	—	6%
DC1-ARC1	Archive Node	—	—	1%
DC1-G1	Gateway Node	—	—	3%
DC1-S1	Storage Node	0%	0%	6%
DC1-S2	Storage Node	0%	0%	8%
DC1-S3	Storage Node	0%	0%	4%
DC2	Site	0%	0%	—


La tabella Nodes (nodi) elenca tutti i siti e i nodi nel sistema StorageGRID. Vengono visualizzate informazioni di riepilogo per ciascun nodo. Se un nodo ha un avviso attivo, viene visualizzata un'icona accanto al nome del nodo. Se il nodo è connesso e non sono presenti avvisi attivi, non viene visualizzata alcuna icona.

Icone di stato della connessione

- Non connesso - Sconosciuto** : Il nodo non è connesso alla rete per un motivo sconosciuto. Ad esempio, la connessione di rete tra i nodi è stata persa o l'alimentazione è inattiva. Potrebbe essere attivato anche l'avviso **Impossibile comunicare con il nodo**. Potrebbero essere attivi anche altri avvisi. Questa situazione richiede un'attenzione immediata.






Un nodo potrebbe apparire come sconosciuto durante le operazioni di shutdown gestite. In questi casi, è possibile ignorare lo stato Unknown (Sconosciuto).

- Non connesso - amministrazione non attiva** : Il nodo non è connesso alla rete per un motivo previsto. Ad esempio, il nodo o i servizi sul nodo sono stati normalmente spenti, il nodo è in fase di riavvio o il software è in fase di aggiornamento. Potrebbero essere attivi anche uno o più avvisi.

Se un nodo viene disconnesso dalla griglia, potrebbe essere visualizzato un avviso sottostante, ma viene visualizzata solo l'icona "non connesso". Per visualizzare gli avvisi attivi per un nodo, selezionare il nodo.

Icone di avviso

Se è presente un avviso attivo per un nodo, accanto al nome del nodo viene visualizzata una delle seguenti icone:

- **Critico** : Si verifica una condizione anomala che ha interrotto le normali operazioni di un nodo o servizio StorageGRID. È necessario risolvere immediatamente il problema sottostante. Se il problema non viene risolto, potrebbero verificarsi interruzioni del servizio e perdita di dati.
- **Maggiore** : Si verifica una condizione anomala che influisce sulle operazioni correnti o si avvicina alla soglia per un avviso critico. È necessario analizzare gli avvisi principali e risolvere eventuali problemi sottostanti per assicurarsi che le condizioni anomale non interrompano il normale funzionamento di un nodo o servizio StorageGRID.
- **Minore** : Il sistema funziona normalmente, ma si verifica una condizione anomala che potrebbe influire sulla capacità di funzionamento del sistema se continua a funzionare. È necessario monitorare e risolvere gli avvisi minori che non vengono risolti da soli per assicurarsi che non causino problemi più gravi.

Dettagli di un sistema, sito o nodo

Per visualizzare le informazioni disponibili, selezionare il nome della griglia, del sito o del nodo nel modo seguente:

- Selezionare il nome della griglia per visualizzare un riepilogo aggregato delle statistiche per l'intero sistema StorageGRID. (La schermata mostra un sistema denominato implementazione StorageGRID).
- Selezionare un sito specifico del data center per visualizzare un riepilogo aggregato delle statistiche per tutti i nodi del sito.
- Selezionare un nodo specifico per visualizzare informazioni dettagliate relative a tale nodo.

Schede per la pagina nodi

Le schede nella parte superiore della pagina nodi si basano su ciò che si seleziona dalla struttura a sinistra.

Nome scheda	Descrizione	Incluso per
Panoramica	<ul style="list-style-type: none"> • Fornisce informazioni di base su ciascun nodo. • Mostra gli avvisi attivi che influiscono sul nodo. 	Tutti i nodi
Hardware	<ul style="list-style-type: none"> • Visualizza l'utilizzo della CPU e della memoria per ciascun nodo • Per i nodi appliance, fornisce informazioni aggiuntive sull'hardware. 	Tutti i nodi
Rete	Visualizza un grafico che mostra il traffico di rete ricevuto e inviato attraverso le interfacce di rete. La vista di un singolo nodo mostra informazioni aggiuntive per il nodo.	Tutti i nodi, ciascun sito e l'intero grid
Storage	<ul style="list-style-type: none"> • Fornisce informazioni dettagliate sui dischi e sui volumi su ciascun nodo. • Per i nodi di storage, ogni sito e l'intero grid include grafici che mostrano lo storage dei dati a oggetti e lo storage dei metadati utilizzati nel tempo. 	Tutti i nodi, ciascun sito e l'intero grid

Nome scheda	Descrizione	Incluso per
Oggetti	<ul style="list-style-type: none"> Fornisce informazioni sulle velocità di acquisizione e recupero di S3 e Swift. Per i nodi di storage, fornisce conteggi di oggetti e informazioni sulle query dell'archivio di metadati e sulla verifica in background. 	Nodi di storage, ciascun sito e l'intero grid
ILM	<p>Fornisce informazioni sulle operazioni ILM (Information Lifecycle Management).</p> <ul style="list-style-type: none"> Per i nodi di storage, fornisce dettagli sulla valutazione ILM e sulla verifica in background per l'eliminazione degli oggetti codificati. Per ogni sito e per l'intera griglia, mostra un grafico della coda ILM nel tempo. Per l'intera griglia, fornisce il tempo stimato per completare una scansione ILM completa di tutti gli oggetti. 	Nodi di storage, ciascun sito e l'intero grid
Bilanciamento del carico	<p>Include grafici diagnostici e relativi alle performance del servizio Load Balancer.</p> <ul style="list-style-type: none"> Per ogni sito, fornisce un riepilogo aggregato delle statistiche per tutti i nodi del sito. Per l'intero grid, fornisce un riepilogo aggregato delle statistiche per tutti i siti. 	Nodi di amministrazione e nodi gateway, ciascun sito e l'intero grid
Servizi della piattaforma	Fornisce informazioni sulle operazioni di servizio della piattaforma S3 in un sito.	Ogni sito
Gestore di sistema di SANtricity	Fornisce l'accesso a Gestione di sistema di SANtricity. Da Gestore di sistema di SANtricity, è possibile esaminare le informazioni ambientali e di diagnostica hardware per il controller di storage, nonché i problemi relativi ai dischi.	<p>Nodi di appliance di storage</p> <p>Nota: La scheda Gestore di sistema di SANtricity non viene visualizzata se il firmware del controller sul dispositivo di storage è precedente alla 8.70 (11.70).</p>

Metriche Prometheus

Il servizio Prometheus sui nodi di amministrazione raccoglie le metriche delle serie temporali dai servizi su tutti i nodi.

Le metriche raccolte da Prometheus vengono utilizzate in diversi punti del Grid Manager:

- **Pagina nodi:** I grafici e i grafici nelle schede disponibili nella pagina nodi utilizzano lo strumento di

visualizzazione Grafana per visualizzare le metriche delle serie temporali raccolte da Prometheus. Grafana visualizza i dati delle serie temporali in formato grafico e grafico, mentre Prometheus funge da origine dei dati back-end.



- **Avvisi:** Gli avvisi vengono attivati a livelli di severità specifici quando le condizioni delle regole di avviso che utilizzano le metriche Prometheus valutano come vero.
- **API per la gestione dei grid:** Puoi utilizzare le metriche Prometheus in regole di avviso personalizzate o con strumenti di automazione esterni per monitorare il tuo sistema StorageGRID. Un elenco completo delle metriche Prometheus è disponibile nell'API Grid Management. (Dalla parte superiore di Grid Manager, selezionare l'icona della guida e selezionare **documentazione API metriche**.) Sebbene siano disponibili più di mille metriche, per monitorare le operazioni StorageGRID più critiche è necessario solo un numero relativamente ridotto.



Le metriche che includono *private* nei loro nomi sono destinate esclusivamente all'uso interno e sono soggette a modifiche tra le release di StorageGRID senza preavviso.

- La pagina **SUPPORT Tools Diagnostics** e la pagina **SUPPORT Tools Metrics**: Queste pagine, destinate principalmente al supporto tecnico, forniscono una serie di tool e grafici che utilizzano i valori delle metriche Prometheus.



Alcune funzioni e voci di menu della pagina metriche sono intenzionalmente non funzionali e sono soggette a modifiche.

Attributi StorageGRID

Gli attributi riportano valori e stati per molte delle funzioni del sistema StorageGRID. I valori degli attributi sono disponibili per ciascun nodo della griglia, per ciascun sito e per l'intera griglia.

Gli attributi StorageGRID vengono utilizzati in diverse posizioni del gestore griglia:

- **Pagina Nodes:** Molti dei valori mostrati nella pagina Nodes sono attributi StorageGRID. (Le metriche Prometheus sono visualizzate anche nelle pagine dei nodi).
- **Allarmi:** Quando gli attributi raggiungono valori di soglia definiti, gli allarmi StorageGRID (sistema legacy) vengono attivati a livelli di severità specifici.
- **Grid Topology tree:** I valori degli attributi vengono visualizzati nell'albero Grid Topology (**SUPPORT Tools Grid Topology**).

- **Eventi:** Gli eventi di sistema si verificano quando alcuni attributi registrano una condizione di errore o di errore per un nodo, inclusi errori come gli errori di rete.

Valori degli attributi

Gli attributi vengono riportati con il massimo sforzo e sono approssimativamente corretti. In alcuni casi, gli aggiornamenti degli attributi possono andare persi, ad esempio il crash di un servizio o il guasto e la ricostruzione di un nodo di rete.

Inoltre, i ritardi di propagazione potrebbero rallentare il reporting degli attributi. I valori aggiornati per la maggior parte degli attributi vengono inviati al sistema StorageGRID a intervalli fissi. Possono essere necessari alcuni minuti prima che un aggiornamento sia visibile nel sistema e due attributi che cambiano più o meno contemporaneamente possono essere riportati in momenti leggermente diversi.

Informazioni correlate

- [Monitorare e risolvere i problemi](#)
- [Monitorare e gestire gli avvisi](#)
- [Utilizzare le opzioni di supporto di StorageGRID](#)

Monitorare e gestire gli avvisi

Il sistema di avviso fornisce un'interfaccia di facile utilizzo per rilevare, valutare e risolvere i problemi che possono verificarsi durante il funzionamento di StorageGRID.

Il sistema di allerta è progettato per essere lo strumento principale per il monitoraggio di eventuali problemi che potrebbero verificarsi nel sistema StorageGRID.

- Il sistema di allerta si concentra su problemi pratici nel sistema. Gli avvisi vengono attivati per gli eventi che richiedono l'attenzione immediata dell'utente, non per gli eventi che possono essere ignorati in modo sicuro.
- Le pagine Avvisi correnti e Avvisi risolti forniscono un'interfaccia intuitiva per la visualizzazione dei problemi correnti e storici. È possibile ordinare l'elenco in base a singoli avvisi e gruppi di avvisi. Ad esempio, è possibile ordinare tutti gli avvisi per nodo/sito per visualizzare gli avvisi che interessano un nodo specifico. In alternativa, è possibile ordinare gli avvisi in un gruppo in base all'ora attivata per trovare l'istanza più recente di un avviso specifico.
- Più avvisi dello stesso tipo sono raggruppati in un'e-mail per ridurre il numero di notifiche. Inoltre, nelle pagine Avvisi correnti e Avvisi risolti vengono visualizzati più avvisi dello stesso tipo come gruppo. È possibile espandere e comprimere i gruppi di avvisi per mostrare o nascondere i singoli avvisi. Ad esempio, se diversi nodi segnalano l'avviso **Impossibile comunicare con il nodo**, viene inviata una sola e-mail e l'avviso viene visualizzato come gruppo nella pagina Avvisi correnti.

View the current alerts affecting your StorageGRID system.

							<input checked="" type="checkbox"/> Group alerts	Active ▼
Name	Severity	Time triggered	Site / Node	Status	Current values			
Unable to communicate with node One or more services are unresponsive or cannot be reached by the metrics collection job.	2 Major	9 minutes ago (newest) 19 minutes ago (oldest)		2 Active				
Low root disk capacity The space available on the root disk is low.	Minor	25 minutes ago	Data Center 1 / DC1-S1-99-51	Active	Disk space available: 2.00 GB Total disk space: 21.00 GB			
Expiration of server certificate for Storage API Endpoints The server certificate used for the storage API endpoints is about to expire.	Major	31 minutes ago	Data Center 1 / DC1-ADM1-99-49	Active	Days remaining: 14			
Expiration of server certificate for Management Interface The server certificate used for the management interface is about to expire.	Minor	31 minutes ago	Data Center 1 / DC1-ADM1-99-49	Active	Days remaining: 30			
Low installed node memory The amount of installed memory on a node is low.	8 Critical	a day ago (newest) a day ago (oldest)		8 Active				

- Gli avvisi utilizzano nomi e descrizioni intuitivi per comprendere più rapidamente il problema. Le notifiche di avviso includono dettagli sul nodo e sul sito interessati, la severità dell'avviso, l'ora in cui è stata attivata la regola di avviso e il valore corrente delle metriche correlate all'avviso.
- Le notifiche e-mail degli avvisi e gli elenchi degli avvisi presenti nelle pagine Avvisi correnti e Avvisi risolti forniscono le azioni consigliate per la risoluzione di un avviso. Queste azioni consigliate spesso includono collegamenti diretti alla documentazione di StorageGRID per semplificare la ricerca e l'accesso a procedure di risoluzione dei problemi più dettagliate.

Low installed node memory

The amount of installed memory on a node is low.

Recommended actions

Increase the amount of RAM available to the virtual machine or Linux host. Check the threshold value for the major alert to determine the default minimum requirement for a StorageGRID node.

See the instructions for your platform:

- [VMware installation](#)
- [Red Hat Enterprise Linux or CentOS installation](#)
- [Ubuntu or Debian installation](#)

Status

Active ([silence this alert](#) [🔗](#))

Site / Node

Data Center 2 / DC2-S1-99-56

Severity

🔴 Critical

Total RAM size

8.38 GB

Condition

[View conditions](#) | [Edit rule](#) [🔗](#)

Time triggered

2019-07-15 17:07:41 MDT (2019-07-15 23:07:41 UTC)

Close



Il sistema di allarme legacy è obsoleto. L'interfaccia utente e le API per il sistema di allarme legacy verranno rimosse in una release futura. Il sistema di allerta offre vantaggi significativi ed è più semplice da utilizzare.

Gestire gli avvisi

Tutti gli utenti di StorageGRID possono visualizzare gli avvisi. Se si dispone dell'autorizzazione Root Access o Manage Alerts (Gestisci avvisi), è possibile gestire gli avvisi anche come segue:

- Se è necessario sospendere temporaneamente le notifiche per un avviso a uno o più livelli di severità, è possibile disattivare facilmente una regola di avviso specifica per un periodo di tempo specificato. È possibile tacitare una regola di avviso per l'intera griglia, un singolo sito o un singolo nodo.
- È possibile modificare le regole di avviso predefinite in base alle esigenze. È possibile disattivare completamente una regola di avviso o modificarne le condizioni di attivazione e la durata.
- È possibile creare regole di avviso personalizzate per definire le condizioni specifiche pertinenti alla situazione e per fornire le azioni consigliate. Per definire le condizioni per un avviso personalizzato, creare espressioni utilizzando le metriche Prometheus disponibili nella sezione metriche dell'API Grid Management.

Ad esempio, questa espressione attiva un avviso se la quantità di RAM installata per un nodo è inferiore a 24,000,000,000 byte (24 GB).

```
node_memory_MemTotal < 24000000000
```

Informazioni correlate

[Monitorare e risolvere i problemi](#)

Utilizzare il monitoraggio SNMP

Se si desidera monitorare StorageGRID utilizzando il protocollo SNMP (Simple Network Management Protocol), è possibile configurare l'agente SNMP utilizzando Grid Manager.

Ogni nodo StorageGRID esegue un agente SNMP, o daemon, che fornisce una base di informazioni di gestione (MIB). Il MIB StorageGRID contiene definizioni di tabella e notifica per avvisi e allarmi. Ogni nodo StorageGRID supporta anche un sottoinsieme di oggetti MIB-II.

Inizialmente, SNMP viene disattivato su tutti i nodi. Quando si configura l'agente SNMP, tutti i nodi StorageGRID ricevono la stessa configurazione.

L'agente SNMP StorageGRID supporta tutte e tre le versioni del protocollo SNMP. L'agente fornisce accesso MIB di sola lettura per le query e può inviare due tipi di notifiche basate sugli eventi a un sistema di gestione:

- **Trap** sono notifiche inviate dall'agente SNMP che non richiedono un riconoscimento da parte del sistema di gestione. Le trap servono a notificare al sistema di gestione che si è verificato qualcosa all'interno di StorageGRID, ad esempio un avviso attivato. I trap sono supportati in tutte e tre le versioni di SNMP.
- Le informazioni * sono simili alle trap, ma richiedono un riconoscimento da parte del sistema di gestione. Se l'agente SNMP non riceve una conferma entro un determinato periodo di tempo, invia nuovamente l'informazione fino a quando non viene ricevuta una conferma o non viene raggiunto il valore massimo di ripetizione. Le informazioni sono supportate in SNMPv2c e SNMPv3.

Le notifiche trap e inform vengono inviate nei seguenti casi:

- Viene attivato un avviso predefinito o personalizzato a qualsiasi livello di severità. Per eliminare le notifiche SNMP per un avviso, è necessario configurare un silenzio per l'avviso. Le notifiche di avviso vengono inviate da qualsiasi nodo amministrativo configurato come mittente preferito.
- Alcuni allarmi (sistema legacy) vengono attivati a livelli di severità specificati o superiori.



Le notifiche SNMP non vengono inviate per ogni allarme o per ogni severità di allarme.

Informazioni correlate

- [Monitorare e risolvere i problemi](#)

Esaminare i messaggi di audit

I messaggi di audit possono aiutarti a comprendere meglio le operazioni dettagliate del tuo sistema StorageGRID. È possibile utilizzare i registri di audit per risolvere i problemi e valutare le performance.

Durante il normale funzionamento del sistema, tutti i servizi StorageGRID generano messaggi di audit, come segue:

- I messaggi di audit del sistema sono correlati al sistema di audit stesso, agli stati dei nodi della griglia, all'attività delle attività a livello di sistema e alle operazioni di backup del servizio.
- I messaggi di audit dello storage a oggetti sono correlati allo storage e alla gestione degli oggetti all'interno di StorageGRID, tra cui storage a oggetti e recuperi, trasferimenti da grid-node a grid-node e verifiche.
- I messaggi di controllo in lettura e scrittura del client vengono registrati quando un'applicazione client S3 o Swift richiede di creare, modificare o recuperare un oggetto.
- I messaggi di controllo della gestione registrano le richieste degli utenti all'API di gestione.

Ogni nodo amministrativo memorizza i messaggi di audit in file di testo. La condivisione dell'audit contiene il file attivo (audit.log) e i registri di audit compressi dei giorni precedenti. Inoltre, ciascun nodo della griglia memorizza una quantità limitata di messaggi di controllo in un file di log locale (localaudit.log).

Per un facile accesso ai registri di audit, è possibile configurare l'accesso client alla condivisione di audit sia per NFS che per CIFS (CIFS è obsoleto). È inoltre possibile accedere ai file di log di audit direttamente dalla riga di comando del nodo di amministrazione.

In alternativa, è possibile inviare le informazioni di audit memorizzate nei nodi Admin e nei nodi locali a un server syslog esterno. L'utilizzo di un server syslog esterno può semplificare la gestione delle informazioni di controllo e ridurre il traffico di rete. Vedere [Configurare i messaggi di audit e le destinazioni dei log](#) per ulteriori informazioni.

Per informazioni dettagliate sul file di log di audit, sul formato dei messaggi di audit, sui tipi di messaggi di audit e sugli strumenti disponibili per analizzare i messaggi di audit, vedere [istruzioni per i messaggi di audit](#). Per informazioni su come configurare l'accesso client di controllo, vedere [Configurare l'accesso al client di audit](#).

Informazioni correlate

- [Esaminare i registri di audit](#)
- [Amministrare StorageGRID](#)

Eseguire la manutenzione

È possibile eseguire diverse procedure di manutenzione per mantenere aggiornato il sistema StorageGRID e garantirne l'efficienza. Grid Manager offre strumenti e opzioni per facilitare il processo di esecuzione delle attività di manutenzione.

Aggiornamenti software

È possibile eseguire tre tipi di aggiornamenti software dalla pagina Software Update in Grid Manager:

- Aggiornamento del software StorageGRID
- Hotfix StorageGRID
- Aggiornamento del sistema operativo SANtricity

Aggiornamenti del software StorageGRID

Quando è disponibile una nuova versione di StorageGRID Feature, la pagina aggiornamento software guida l'utente attraverso il processo di caricamento del file richiesto e l'aggiornamento del sistema StorageGRID. È necessario aggiornare tutti i nodi grid per tutti i siti del data center dal nodo di amministrazione primario.

Durante un aggiornamento del software StorageGRID, le applicazioni client possono continuare ad acquisire e recuperare i dati degli oggetti.

Hotfix

Se i problemi relativi al software vengono rilevati e risolti tra una versione e l'altra, potrebbe essere necessario applicare una correzione rapida al sistema StorageGRID.

Le hotfix StorageGRID contengono modifiche software rese disponibili al di fuori di una release di funzionalità o patch. Le stesse modifiche sono incluse in una release futura.

La pagina Hotfix di StorageGRID, illustrata di seguito, consente di caricare un file hotfix.

StorageGRID Hotfix

Before starting the hotfix process, you must confirm that there are no active alerts and that all grid nodes are online and available.

When the primary Admin Node is updated, services are stopped and restarted. Connectivity might be interrupted until the services are back online.

Hotfix file

Hotfix file ?

Browse

Passphrase

Provisioning Passphrase ?

Start

La correzione rapida viene applicata per prima al nodo di amministrazione primario. Quindi, è necessario approvare l'applicazione della correzione rapida ad altri nodi della griglia fino a quando tutti i nodi nel sistema StorageGRID non eseguono la stessa versione software. È possibile personalizzare la sequenza di approvazione selezionando per approvare singoli nodi della griglia, gruppi di nodi della griglia o tutti i nodi della griglia.



Mentre tutti i nodi della griglia vengono aggiornati con la nuova versione di hotfix, le modifiche effettive di una hotfix potrebbero interessare solo servizi specifici su tipi specifici di nodi. Ad esempio, una correzione rapida potrebbe influire solo sul servizio LDR sui nodi di storage.

Aggiornamenti del sistema operativo SANtricity

Se i controller non funzionano in modo ottimale, potrebbe essere necessario aggiornare il software SANtricity OS sui controller storage delle appliance di storage. È possibile caricare il file del sistema operativo SANtricity nel nodo di amministrazione principale del sistema StorageGRID e applicare l'aggiornamento da Gestione griglia.

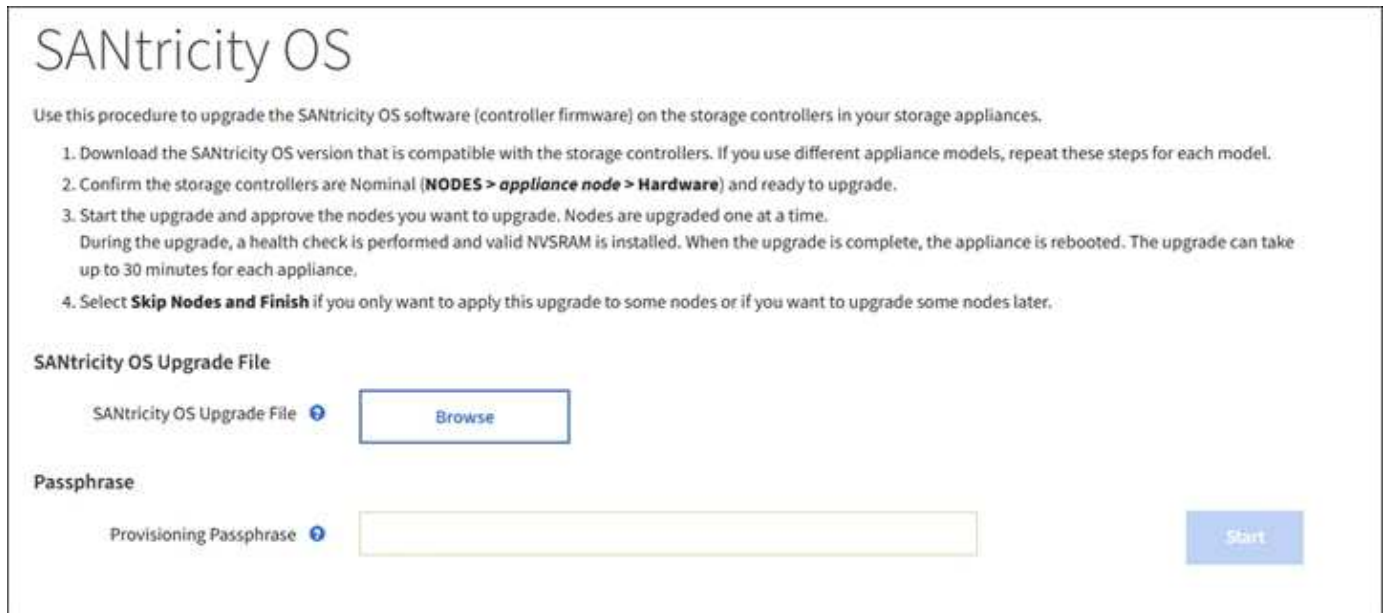
La pagina SANtricity, illustrata di seguito, consente di caricare il file di aggiornamento del sistema operativo SANtricity.

SANtricity OS


Use this procedure to upgrade the SANtricity OS software (controller firmware) on the storage controllers in your storage appliances.

1. Download the SANtricity OS version that is compatible with the storage controllers. If you use different appliance models, repeat these steps for each model.
2. Confirm the storage controllers are Nominal (**NODES > appliance node > Hardware**) and ready to upgrade.
3. Start the upgrade and approve the nodes you want to upgrade. Nodes are upgraded one at a time.
During the upgrade, a health check is performed and valid NVSRAM is installed. When the upgrade is complete, the appliance is rebooted. The upgrade can take up to 30 minutes for each appliance.
4. Select **Skip Nodes and Finish** if you only want to apply this upgrade to some nodes or if you want to upgrade some nodes later.

SANtricity OS Upgrade File

SANtricity OS Upgrade File 

Passphrase

Provisioning Passphrase 

Dopo aver caricato il file, è possibile approvare l'aggiornamento su singoli nodi di storage o su tutti i nodi. La possibilità di approvare i nodi in modo selettivo semplifica la pianificazione dell'aggiornamento. Dopo aver approvato un nodo per l'aggiornamento, il sistema esegue un controllo dello stato di salute e installa l'aggiornamento, se applicabile al nodo.

Procedure di espansione

È possibile espandere un sistema StorageGRID aggiungendo volumi di storage ai nodi storage, aggiungendo nuovi nodi grid a un sito esistente o aggiungendo un nuovo sito del data center. Se si dispone di nodi di storage che utilizzano l'appliance di storage SG6060 o SG6060X, è possibile aggiungere uno o due shelf di espansione per raddoppiare o triplicare la capacità di storage del nodo.

È possibile eseguire espansioni senza interrompere il funzionamento del sistema corrente. Quando si aggiungono nodi o un sito, si distribuiscono i nuovi nodi e quindi si esegue la procedura di espansione dalla pagina Grid Expansion.

Grid Expansion

i A new Recovery Package has been generated as a result of the configuration change. Go to the [Recovery Package](#) page to download it.

Expansion Progress

Lists the status of grid configuration tasks required to change the grid topology. These grid configuration tasks are run automatically by the StorageGRID system.

1. Installing Grid Nodes

In Progress

Grid Node Status

Lists the installation and configuration status of each grid node included in the expansion.

Search						Q
Name	Site	Grid Network IPv4 Address	Progress	Stage		
DC2-ADM1-184	Site A	172.17.3.184/21	<div><div></div></div>	Waiting for NTP to synchronize		
DC2-S1-185	Site A	172.17.3.185/21	<div><div></div></div>	Waiting for Dynamic IP Service peers		
DC2-S2-186	Site A	172.17.3.186/21	<div><div></div></div>	Waiting for NTP to synchronize		
DC2-S3-187	Site A	172.17.3.187/21	<div><div></div></div>	Waiting for NTP to synchronize		
DC2-S4-188	Site A	172.17.3.188/21	<div><div></div></div>	Waiting for Dynamic IP Service peers		
DC2-ARC1-189	Site A	172.17.3.189/21	<div><div></div></div>	Waiting for NTP to synchronize		

2. Initial Configuration

Pending

3. Distributing the new grid node's certificates to the StorageGRID system.

Pending

4. Starting services on the new grid nodes

Pending

5. Cleaning up unused Cassandra keys

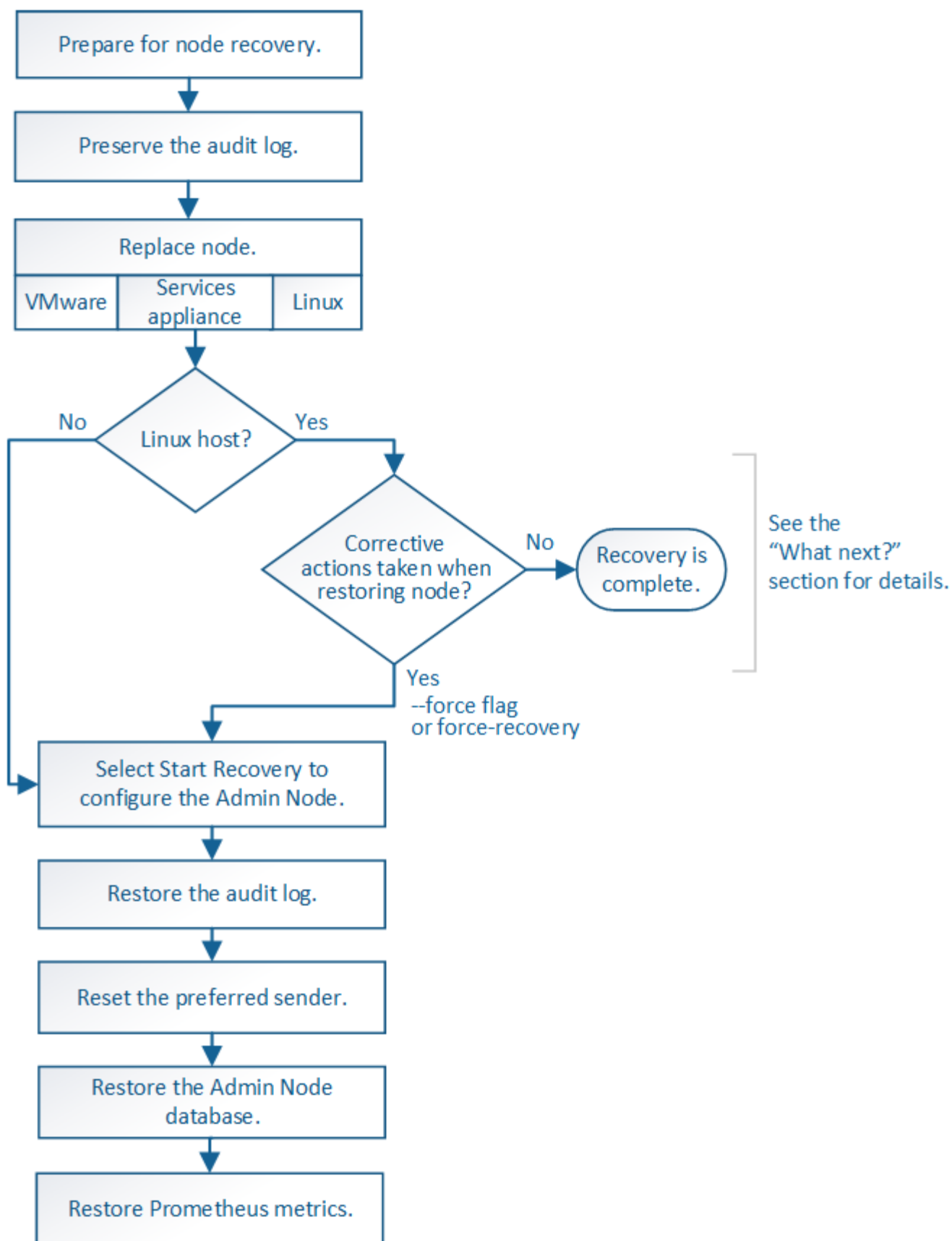
Pending

Procedure di recovery dei nodi

I nodi Grid possono non funzionare se un guasto hardware, virtualizzazione, sistema operativo o software rende il nodo inutilizzabile o inaffidabile.

I passaggi per il ripristino di un nodo grid dipendono dalla piattaforma in cui è ospitato il nodo grid e dal tipo di nodo grid. Ogni tipo di nodo della griglia dispone di una procedura di ripristino specifica, che è necessario seguire con precisione. In genere, se possibile, si tenta di conservare i dati dal nodo della griglia guasto, riparare o sostituire il nodo guasto, utilizzare la pagina Recovery per configurare il nodo sostitutivo e ripristinare i dati del nodo.

Ad esempio, questo diagramma di flusso mostra la procedura di ripristino in caso di guasto di un nodo amministratore.



Procedura di decommissionamento

Si consiglia di rimuovere in modo permanente i nodi grid o un intero sito del data center dal sistema StorageGRID.

Ad esempio, potrebbe essere necessario decommissionare uno o più nodi di rete nei seguenti casi:

- È stato aggiunto un nodo di storage più grande al sistema e si desidera rimuovere uno o più nodi di storage più piccoli, preservando al contempo gli oggetti.
- Richiede meno storage totale.
- Non è più necessario un nodo gateway o un nodo amministratore non primario.
- La griglia include un nodo disconnesso che non è possibile ripristinare o ripristinare online.

È possibile utilizzare la pagina Decommission Nodes in Grid Manager per rimuovere i seguenti tipi di nodi griglia:

- Nodi di storage, a meno che non resti un numero sufficiente di nodi nel sito per supportare determinati requisiti
- Nodi gateway
- Nodi amministrativi non primari

Decommission Nodes

Before decommissioning a grid node, review the health of all nodes. If possible, resolve any issues or alarms before proceeding.

Select the checkbox for each grid node you want to decommission. If decommission is not possible for a node, see the Recovery and Maintenance Guide to learn how to proceed.

Grid Nodes

Name	Site	Type	Has ADC	Health	Decommission Possible
DC1-ADM1	Data Center 1	Admin Node	-	✓	No, primary Admin Node decommissioning is not supported.
DC1-ARC1	Data Center 1	Archive Node	-	✓	No, Archive Nodes decommissioning is not supported.
<input type="checkbox"/> DC1-G1	Data Center 1	API Gateway Node	-	✓	✓
DC1-S1	Data Center 1	Storage Node	Yes	✓	No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
DC1-S2	Data Center 1	Storage Node	Yes	✓	No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
DC1-S3	Data Center 1	Storage Node	Yes	✓	No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
<input type="checkbox"/> DC1-S4	Data Center 1	Storage Node	No	✓	✓
<input type="checkbox"/> DC2-ADM1	Data Center 2	Admin Node	-	✓	✓
DC2-S1	Data Center 2	Storage Node	Yes	✓	No, site Data Center 2 requires a minimum of 3 Storage Nodes with ADC services.

Per rimuovere un sito, puoi utilizzare la pagina Decommission Site di Grid Manager. La decommissionazione di un sito connesso rimuove un sito operativo e conserva i dati. La decommissionazione di un sito disconnesso rimuove un sito guasto ma non conserva i dati. La procedura guidata Decommission Site guida l'utente nel processo di selezione del sito, visualizzazione dei dettagli del sito, revisione dei criteri ILM, rimozione dei riferimenti del sito dalle regole ILM e risoluzione dei conflitti di nodo.

Decommission Site



When you decommission a site, all nodes at the site and the site itself are permanently removed from the StorageGRID system.

Review the table for the site you want to remove. If Decommission Possible is Yes, select the site. Then, select **Next** to ensure that the site is not referred to by ILM and that all StorageGRID nodes are in the correct state.

You might not be able to remove certain sites. For example, you cannot decommission the site that contains the primary Admin Node or a site that contains an Archive Node.

Sites

	Site Name	Used Storage Capacity ?	Decommission Possible
<input type="radio"/>	Raleigh	3.93 MB	✓
<input type="radio"/>	Sunnyvale	3.97 MB	✓
<input type="radio"/>	Vancouver	3.90 MB	No. This site contains the primary Admin Node.

Next

Procedure di manutenzione della rete

Alcune delle procedure di manutenzione della rete che potrebbe essere necessario eseguire includono quanto segue:

- Aggiornamento delle subnet sulla rete Grid
- Utilizzo dello strumento Change IP per modificare la configurazione di rete inizialmente impostata durante l'implementazione della griglia
- Aggiunta, rimozione o aggiornamento dei server DNS (Domain Name System)
- Aggiunta, rimozione o aggiornamento di server NTP (Network Time Protocol) per garantire la sincronizzazione accurata dei dati tra i nodi di rete
- Ripristino della connettività di rete ai nodi che potrebbero essere stati isolati dal resto della griglia

Procedure middleware e a livello di host

Alcune procedure di manutenzione sono specifiche per i nodi StorageGRID implementati su Linux o VMware oppure sono specifiche di altri componenti della soluzione StorageGRID. Ad esempio, è possibile eseguire la migrazione di un nodo grid a un host Linux diverso o la manutenzione su un nodo di archiviazione connesso a Tivoli Storage Manager (TSM).

Cloning del nodo dell'appliance

Il cloning dei nodi dell'appliance consente di sostituire facilmente un nodo dell'appliance esistente nel grid con un'appliance dal design più recente o con funzionalità avanzate che fanno parte dello stesso sito StorageGRID logico. Il processo trasferisce tutti i dati alla nuova appliance, mettendola in servizio per sostituire il nodo della vecchia appliance e lasciandola in uno stato pre-installato. La clonazione offre un processo di aggiornamento dell'hardware semplice da eseguire e un metodo alternativo per la sostituzione delle appliance.

Procedure del nodo di rete

Potrebbe essere necessario eseguire alcune procedure su un nodo della griglia specifico. Ad esempio, potrebbe essere necessario riavviare un nodo di rete o arrestare e riavviare manualmente un servizio di nodo di rete specifico. È possibile eseguire alcune procedure dei nodi della griglia da Grid Manager; altre richiedono l'accesso al nodo della griglia e l'utilizzo della riga di comando del nodo.

Informazioni correlate

- [Amministrare StorageGRID](#)
- [Aggiornare il software](#)
- [Espandi il tuo grid](#)
- [Ripristino e manutenzione](#)

Scaricare il pacchetto di ripristino

Il pacchetto di ripristino è un file .zip scaricabile che contiene file e software specifici per l'implementazione necessari per installare, espandere, aggiornare e gestire un sistema StorageGRID.

Il file Recovery Package contiene anche informazioni di configurazione e integrazione specifiche del sistema, inclusi nomi host e indirizzi IP dei server, nonché password altamente riservate necessarie durante la manutenzione, l'aggiornamento e l'espansione del sistema. Il pacchetto di ripristino è necessario per eseguire il ripristino in caso di guasto del nodo di amministrazione primario.

Quando si installa un sistema StorageGRID, è necessario scaricare il file del pacchetto di ripristino e confermare che è possibile accedere al contenuto del file. È inoltre necessario scaricare il file ogni volta che la topologia della griglia del sistema StorageGRID cambia a causa delle procedure di manutenzione o aggiornamento.

Recovery Package

Enter your provisioning passphrase and click Start Download to save a copy of the Recovery Package file. Download the file each time the grid topology of the StorageGRID system changes because of maintenance or upgrade procedures, so that you can restore the grid if a failure occurs.

When the download completes, copy the Recovery Package file to two safe, secure, and separate locations.

Important: The Recovery Package file must be secured because it contains encryption keys and passwords that can be used to obtain data from the StorageGRID system.

Provisioning Passphrase

Start Download

Dopo aver scaricato il file del pacchetto di ripristino e aver confermato che è possibile estrarre il contenuto, copiare il file del pacchetto di ripristino 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.

Informazioni correlate

- [Aggiornare il software](#)
- [Espandi il tuo grid](#)

- [Ripristino e manutenzione](#)

Utilizzare le opzioni di supporto di StorageGRID

Grid Manager offre opzioni per aiutarti a lavorare con il supporto tecnico in caso di problemi con il tuo sistema StorageGRID.

Configurare AutoSupport

La funzione AutoSupport consente al sistema StorageGRID di inviare messaggi di stato e di stato al supporto tecnico. L'utilizzo di AutoSupport può accelerare notevolmente la determinazione e la risoluzione dei problemi. Il supporto tecnico può anche monitorare le esigenze di storage del sistema e aiutare a determinare se è necessario aggiungere nuovi nodi o siti. In alternativa, è possibile configurare i messaggi AutoSupport in modo che vengano inviati a una destinazione aggiuntiva.

Si configura AutoSupport utilizzando il gestore di griglia (**SUPPORT Tools AutoSupport**). La pagina **AutoSupport** contiene due schede: **Impostazioni** e **risultati**.

AutoSupport

The AutoSupport feature enables your StorageGRID system to send periodic and event-driven health and status messages to technical support to allow proactive monitoring and troubleshooting. StorageGRID AutoSupport also enables the use of Active IQ for predictive recommendations.

Settings

Results

Protocol Details

Protocol ?
☒ HTTPS ☐ HTTP ☐ SMTP

NetApp Support Certificate Validation ?

Use NetApp support certificate

AutoSupport Details

Enable Weekly AutoSupport ? ☒

Enable Event-Triggered AutoSupport ? ☒

Enable AutoSupport on Demand ? ☐

Software Updates

Check for software updates ? ☒

Additional AutoSupport Destination

Enable Additional AutoSupport Destination ? ☐

Save

Send User-Triggered AutoSupport

Informazioni incluse nei messaggi AutoSupport

I messaggi AutoSupport includono informazioni quali:

- Versione del software StorageGRID
- Versione del sistema operativo

- Informazioni sugli attributi a livello di sistema e di posizione
- Avvisi e allarmi recenti (sistema legacy)
- Stato corrente di tutte le attività della griglia, inclusi i dati storici
- Utilizzo del database Admin Node
- Numero di oggetti persi o mancanti
- Impostazioni di configurazione della griglia
- Entità NMS
- Policy ILM attiva
- File delle specifiche della griglia con provisioning
- Metriche diagnostiche

È possibile attivare la funzione AutoSupport e le singole opzioni AutoSupport quando si installa StorageGRID per la prima volta oppure attivarle in un secondo momento. Se AutoSupport non è attivato, viene visualizzato un messaggio nella dashboard di Grid Manager. Il messaggio include un collegamento alla pagina di configurazione di AutoSupport.

The AutoSupport feature is disabled. You should [enable AutoSupport](#) to allow StorageGRID to send health and status messages to technical support for proactive monitoring and troubleshooting.



Se si chiude il messaggio, questo non viene visualizzato fino a quando la cache del browser non viene cancellata, anche se AutoSupport rimane disattivato.

USA Active IQ

Active IQ è un consulente digitale basato sul cloud che sfrutta l'analisi predittiva e la saggezza della community della base installata di NetApp. Le valutazioni continue dei rischi, gli avvisi predittivi, le indicazioni prescrittive e le azioni automatizzate consentono di prevenire i problemi prima che si verifichino, migliorando lo stato di salute del sistema e la disponibilità del sistema.

Se si desidera utilizzare le dashboard e le funzionalità di Active IQ sul sito del supporto, è necessario attivare AutoSupport.

["Documentazione di Active IQ Digital Advisor"](#)

Raccogliere i log StorageGRID

Per risolvere un problema, potrebbe essere necessario raccogliere i file di log e inoltrarli al supporto tecnico.

StorageGRID utilizza i file di registro per acquisire eventi, messaggi di diagnostica e condizioni di errore. Il file bycast.log viene gestito per ogni nodo grid ed è il file principale per la risoluzione dei problemi. StorageGRID crea inoltre file di log per i singoli servizi StorageGRID, file di log relativi alle attività di implementazione e manutenzione e file di log relativi alle applicazioni di terze parti.

Gli utenti che dispongono delle autorizzazioni appropriate e conoscono la passphrase di provisioning per il sistema StorageGRID possono utilizzare la pagina registri di Gestione griglia per raccogliere file di log, dati di sistema e dati di configurazione. Quando si raccolgono i registri, selezionare uno o più nodi e specificare un periodo di tempo. I dati vengono raccolti e archiviati in un `.tar.gz` che è possibile scaricare su un computer

locale. All'interno di questo file è presente un archivio di file di log per ciascun nodo della griglia.

StorageGRID

- DC1
 - DC1-ADM1
 - DC1-G1
 - DC1-S1
 - DC1-S2
 - DC1-S3
 - DC1-S4
- DC2
 - DC2-ADM1
 - DC2-G1
 - DC2-S1
 - DC2-S2
 - DC2-S3
 - DC2-S4

Log Start Time: 2021-12-03 06:31 AM MST

Log End Time: 2021-12-03 10:31 AM MST

Log Types: ☒ Application Logs, ☐ Network Trace, ☐ Audit Logs, ☐ Prometheus Database

Notes: [Empty text area]

Provisioning Passphrase: [Masked field]

Collect Logs

Utilizzare le metriche ed eseguire la diagnostica

Durante la risoluzione di un problema, puoi lavorare con il supporto tecnico per rivedere metriche e grafici dettagliati per il tuo sistema StorageGRID. È inoltre possibile eseguire query diagnostiche precostruite per valutare in modo proattivo i valori chiave per il sistema StorageGRID.

Pagina Metrics (metriche)

La pagina metriche consente di accedere alle interfacce utente Prometheus e Grafana. Prometheus è un software open-source per la raccolta di metriche. Grafana è un software open-source per la visualizzazione delle metriche.



Gli strumenti disponibili nella pagina metriche sono destinati all'utilizzo da parte del supporto tecnico. Alcune funzioni e voci di menu di questi strumenti sono intenzionalmente non funzionali e sono soggette a modifiche.

Metrics

Access charts and metrics to help troubleshoot issues.

i The tools available on this page are intended for use by technical support. Some features and menu items within these tools are intentionally non-functional.

Prometheus

Prometheus is an open-source toolkit for collecting metrics. The Prometheus interface allows you to query the current values of metrics and to view charts of the values over time.

Access the Prometheus UI using the link below. You must be signed in to the Grid Manager.

- <https://storagegrid.sageit.com/metrics/graph>

Grafana

Grafana is open-source software for metrics visualization. The Grafana interface provides pre-constructed dashboards that contain graphs of important metric values over time.

Access the Grafana dashboards using the links below. You must be signed in to the Grid Manager.

ADE	Grid	S3 - Node
Account Service Overview	ILM	S3 Overview
Alertmanager	Identity Service Overview	S3 Select
Audit Overview	Ingests	Site
Cassandra Cluster Overview	Node	Support
Cassandra Network Overview	Node (Internal Use)	Traces
Cassandra Node Overview	OSL - AsyncIO	Traffic Classification Policy
Cloud Storage Pool Overview	Platform Services Commits	Usage Processing
EC - ADE	Platform Services Overview	Virtual Memory (vmstat)
EC - Chunk Service	Platform Services Processing	
EC Overview	Replicated Read Path Overview	

Il collegamento nella sezione Prometheus della pagina metriche consente di eseguire query sui valori correnti delle metriche StorageGRID e di visualizzare i grafici dei valori nel tempo.

PrometheusAlertsGraphStatus ▾Help

☐ Enable query history

Expression (press Shift+Enter for newlines)

Execute

- insert metric at cursor - ▾

Graph

Console

Element	Value
no data	

Remove Graph

Add Graph



Le metriche che includono *private* nei loro nomi sono destinate esclusivamente all'uso interno e sono soggette a modifiche tra le release di StorageGRID senza preavviso.

I collegamenti nella sezione Grafana della pagina metriche consentono di accedere ai dashboard predefiniti contenenti grafici delle metriche StorageGRID nel tempo.



Pagina di diagnostica

La pagina Diagnostics (Diagnostica) esegue una serie di controlli diagnostici predefiniti sullo stato corrente della griglia. Nell'esempio, tutte le diagnostiche hanno uno stato normale.

Diagnostics

This page performs a set of diagnostic checks on the current state of the grid. A diagnostic check can have one of three statuses:

- ✓ **Normal:** All values are within the normal range.
- ⚠ **Attention:** One or more of the values are outside of the normal range.
- ✖ **Caution:** One or more of the values are significantly outside of the normal range.

Diagnostic statuses are independent of current alerts and might not indicate operational issues with the grid. For example, a diagnostic check might show Caution status even if no alert has been triggered.

Run Diagnostics

✓ Cassandra blocked task queue too large



✓ Cassandra commit log latency



✓ Cassandra commit log queue depth



✓ Cassandra compaction queue too large



Facendo clic su una diagnostica specifica, è possibile visualizzare i dettagli della diagnostica e dei relativi risultati correnti.

In questo esempio, viene mostrato l'utilizzo corrente della CPU per ogni nodo in un sistema StorageGRID. Tutti i valori dei nodi sono al di sotto delle soglie di attenzione e attenzione, quindi lo stato generale della diagnostica è normale.

CPU utilization

Checks the current CPU utilization on each node.

To view charts of CPU utilization and other per-node metrics, access the [Node Grafana dashboard](#).

Status

Normal

Prometheus query

```
sum by (instance) (sum by (instance, mode) (irate(node_cpu_seconds_total{mode!="idle"}[5m])) / count by (instance, mode)(node_cpu_seconds_total{mode!="idle"}))
```

[View in Prometheus](#)

Thresholds

Attention >= 75%
 Caution >= 95%

Status	Instance	CPU Utilization
	DC1-ADM1	2.598%
	DC1-ARC1	0.937%
	DC1-G1	2.119%
	DC1-S1	8.708%
	DC1-S2	8.142%
	DC1-S3	9.669%
	DC2-ADM1	2.515%
	DC2-ARC1	1.152%
	DC2-S1	8.204%
	DC2-S2	5.000%
	DC2-S3	10.469%

Informazioni correlate

- [Amministrare StorageGRID](#)
- [Configurare le impostazioni di rete](#)

Linee guida per il networking

Linee guida per il networking: Panoramica

Utilizza queste linee guida per conoscere l'architettura StorageGRID e le topologie di rete e per conoscere i requisiti per la configurazione e il provisioning di rete.

A proposito di queste istruzioni

Queste linee guida forniscono informazioni utili per creare l'infrastruttura di rete StorageGRID prima di implementare e configurare i nodi StorageGRID. Utilizzare queste linee guida per garantire che la comunicazione possa avvenire tra tutti i nodi della griglia e tra la griglia e i client e i servizi esterni.

I client esterni e i servizi esterni devono connettersi alle reti StorageGRID per eseguire le seguenti funzioni:

- Memorizzare e recuperare i dati degli oggetti
- Ricevi notifiche via email
- Accedere all'interfaccia di gestione di StorageGRID (il gestore di griglia e il gestore dei tenant)

- Accesso alla condivisione dell'audit (opzionale)
- Fornire servizi come:
 - NTP (Network Time Protocol)
 - DNS (Domain Name System)
 - Server di gestione delle chiavi (KMS)

La rete StorageGRID deve essere configurata in modo appropriato per gestire il traffico per queste funzioni e altro ancora.

Prima di iniziare

La configurazione della rete per un sistema StorageGRID richiede un livello elevato di esperienza con switch Ethernet, reti TCP/IP, subnet, routing di rete e firewall.

Prima di configurare la rete, acquisire familiarità con l'architettura StorageGRID come descritto in [Primer griglia](#).

Dopo aver stabilito quali reti StorageGRID si desidera utilizzare e come configurarle, è possibile installare e configurare i nodi StorageGRID seguendo le istruzioni appropriate.

Installare nodi basati su software

- [Installare Red Hat Enterprise Linux o CentOS](#)
- [Installare Ubuntu o Debian](#)
- [Installare VMware](#)

Installare i nodi appliance

- [Appliance di servizi SG100 e SG1000](#)
- [Appliance di storage SG6000](#)
- [Appliance di storage SG5700](#)
- [Appliance di storage SG5600](#)

Configurare e amministrare il software StorageGRID

- [Amministrare StorageGRID](#)
- [Note di rilascio](#)

Tipi di rete StorageGRID

I nodi della griglia in un sistema StorageGRID elaborano *grid traffic*, *admin traffic* e *client traffic*. È necessario configurare la rete in modo appropriato per gestire questi tre tipi di traffico e fornire controllo e sicurezza.

Tipi di traffico

Tipo di traffico	Descrizione	Tipo di rete
Traffico di rete	Il traffico StorageGRID interno che viaggia tra tutti i nodi della griglia. Tutti i nodi della rete devono essere in grado di comunicare con tutti gli altri nodi della rete.	Grid Network (obbligatorio)
Traffico amministrativo	Il traffico utilizzato per l'amministrazione e la manutenzione del sistema.	Admin Network (opzionale), Rete VLAN (opzionale)
Traffico del client	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.	Rete client (opzionale), Rete VLAN (opzionale)

È possibile configurare la rete nei seguenti modi:

- Solo Grid Network
- Reti Grid e Admin
- Reti grid e client
- Reti Grid, Admin e Client

Grid Network è obbligatorio e può gestire tutto il traffico di rete. Le reti Admin e Client possono essere incluse al momento dell'installazione o aggiunte in un secondo momento per adattarsi alle modifiche dei requisiti. Sebbene la rete amministrativa e la rete client siano opzionali, quando si utilizzano queste reti per gestire il traffico amministrativo e client, la rete griglia può essere resa isolata e sicura.

Le porte interne sono accessibili solo tramite la rete Grid. Le porte esterne sono accessibili da tutti i tipi di rete. Questa flessibilità offre diverse opzioni per la progettazione di un'implementazione StorageGRID e la configurazione di IP esterni e filtraggio delle porte in switch e firewall. Vedere [comunicazioni interne al nodo di rete](#) e [comunicazioni esterne](#).

Interfacce di rete

I nodi StorageGRID sono connessi a ciascuna rete utilizzando le seguenti interfacce specifiche:

Rete	Nome dell'interfaccia
Grid Network (obbligatorio)	eth0
Admin Network (opzionale)	eth1
Rete client (opzionale)	eth2

Per ulteriori informazioni sulla mappatura delle porte fisiche o virtuali alle interfacce di rete dei nodi, consultare le istruzioni di installazione:

Nodi basati su software

- [Installare Red Hat Enterprise Linux o CentOS](#)

- [Installare Ubuntu o Debian](#)
- [Installare VMware](#)

Nodi appliance

- [Appliance di servizi SG100 e SG1000](#)
- [Appliance di storage SG6000](#)
- [Appliance di storage SG5700](#)
- [Appliance di storage SG5600](#)

Informazioni di rete per ciascun nodo

È necessario configurare quanto segue per ogni rete abilitata su un nodo:

- Indirizzo IP
- Subnet mask
- Indirizzo IP del gateway

È possibile configurare una sola combinazione di indirizzo IP/maschera/gateway per ciascuna delle tre reti su ciascun nodo della griglia. Se non si desidera configurare un gateway per una rete, utilizzare l'indirizzo IP come indirizzo del gateway.

Gruppi ad alta disponibilità

I gruppi ad alta disponibilità (ha) consentono di aggiungere indirizzi IP virtuali (VIP) all'interfaccia Grid o Client Network. Per ulteriori informazioni, vedere [Gestire i gruppi ad alta disponibilità](#).

Grid Network

La rete grid è obbligatoria. Viene utilizzato per tutto il traffico StorageGRID interno. Grid Network offre connettività tra tutti i nodi della rete, in tutti i siti e le subnet. Tutti i nodi della rete Grid devono essere in grado di comunicare con tutti gli altri nodi. La rete Grid può essere costituita da più sottoreti. Le reti contenenti servizi grid critici, come NTP, possono essere aggiunte anche come subnet grid.



StorageGRID non supporta NAT (Network Address Translation) tra nodi.

La rete Grid può essere utilizzata per tutto il traffico amministrativo e per tutto il traffico client, anche se sono configurate la rete Admin e la rete client. Il gateway Grid Network è il gateway predefinito del nodo, a meno che il nodo non abbia configurato la rete client.



Quando si configura Grid Network, è necessario assicurarsi che la rete sia protetta da client non attendibili, ad esempio quelli su Internet.

Tenere presente i seguenti requisiti e dettagli per il gateway Grid Network:

- Il gateway Grid Network deve essere configurato se sono presenti più subnet Grid.
- Il gateway Grid Network è il gateway predefinito del nodo fino al completamento della configurazione della griglia.
- Le route statiche vengono generate automaticamente per tutti i nodi a tutte le subnet configurate nell'elenco globale delle subnet di rete Grid.

- Se viene aggiunta una rete client, il gateway predefinito passa dal gateway Grid Network al gateway Client Network una volta completata la configurazione della rete.

Admin Network (rete amministrativa)

La rete di amministrazione è opzionale. Una volta configurato, può essere utilizzato per l'amministrazione del sistema e il traffico di manutenzione. La rete amministrativa è in genere una rete privata e non deve essere instradabile tra i nodi.

È possibile scegliere i nodi della griglia su cui attivare la rete di amministrazione.

Quando si utilizza la rete di amministrazione, non è necessario che il traffico amministrativo e di manutenzione si sposti attraverso la rete di griglia. Gli utilizzi tipici della rete di amministrazione includono:

- Accesso alle interfacce utente di Grid Manager e Tenant Manager.
- Accesso a servizi critici come server NTP, server DNS, server KMS (Key Management Server) esterni e server LDAP (Lightweight Directory Access Protocol).
- Accesso ai registri di controllo sui nodi di amministrazione.
- Accesso SSH (Secure Shell Protocol) per manutenzione e supporto.

La rete amministrativa non viene mai utilizzata per il traffico di rete interno. Viene fornito un gateway Admin Network che consente alla rete di amministrazione di comunicare con più sottoreti esterne. Tuttavia, il gateway Admin Network non viene mai utilizzato come gateway predefinito del nodo.

Tenere presente i seguenti requisiti e dettagli per il gateway Admin Network:

- Il gateway Admin Network è necessario se le connessioni vengono effettuate dall'esterno della subnet Admin Network o se sono configurate più subnet Admin Network.
- Vengono creati percorsi statici per ogni subnet configurata nell'elenco subnet di rete amministrativa del nodo.

Rete client

La rete client è opzionale. Una volta configurato, viene utilizzato per fornire l'accesso ai servizi grid per le applicazioni client come S3 e Swift. Se si prevede di rendere i dati StorageGRID accessibili a una risorsa esterna (ad esempio, un pool di storage cloud o il servizio di replica di StorageGRID), la risorsa esterna può utilizzare anche la rete client. I nodi Grid possono comunicare con qualsiasi subnet raggiungibile tramite il gateway di rete client.

È possibile scegliere i nodi della griglia su cui deve essere attivata la rete client. Non è necessario che tutti i nodi si trovino sulla stessa rete client e i nodi non comunicheranno mai l'uno con l'altro sulla rete client. La rete client non diventa operativa fino al completamento dell'installazione della griglia.

Per una maggiore sicurezza, è possibile specificare che l'interfaccia di rete client di un nodo sia non attendibile in modo che la rete client sia più restrittiva delle connessioni consentite. Se l'interfaccia Client Network di un nodo non è attendibile, l'interfaccia accetta connessioni in uscita come quelle utilizzate dalla replica di CloudMirror, ma accetta solo connessioni in entrata su porte che sono state configurate esplicitamente come endpoint del bilanciamento del carico. Vedere [Gestire reti client non attendibili](#) e [Configurare gli endpoint del bilanciamento del carico](#).

Quando si utilizza una rete client, il traffico client non deve attraversare la rete griglia. Il traffico Grid Network può essere separato su una rete sicura e non instradabile. I seguenti tipi di nodo sono spesso configurati con una rete client:

- Nodi gateway, perché questi nodi forniscono l'accesso al servizio bilanciamento del carico StorageGRID e all'accesso del client S3 e Swift alla griglia.
- Nodi di storage, perché questi nodi forniscono accesso ai protocolli S3 e Swift, ai Cloud Storage Pools e al servizio di replica CloudMirror.
- Nodi di amministrazione, per garantire che gli utenti tenant possano connettersi a tenant Manager senza dover utilizzare la rete di amministrazione.

Tenere presente quanto segue per il gateway di rete client:

- Il gateway di rete client è necessario se la rete client è configurata.
- Una volta completata la configurazione della griglia, il gateway di rete client diventa il percorso predefinito per il nodo della griglia.

Reti VLAN opzionali

Se necessario, è possibile utilizzare reti LAN virtuali (VLAN) per il traffico client e per alcuni tipi di traffico amministrativo. Il traffico di rete, tuttavia, non può utilizzare un'interfaccia VLAN. Il traffico StorageGRID interno tra i nodi deve sempre utilizzare la rete griglia su eth0.

Per supportare l'utilizzo delle VLAN, è necessario configurare una o più interfacce su un nodo come interfacce di trunk sullo switch. È possibile configurare l'interfaccia Grid Network (eth0) o l'interfaccia Client Network (eth2) come trunk oppure è possibile aggiungere interfacce trunk al nodo.

Se eth0 è configurato come trunk, il traffico Grid Network passa attraverso l'interfaccia nativa del trunk, come configurato sullo switch. Analogamente, se eth2 è configurato come trunk e Client Network è configurato sullo stesso nodo, Client Network utilizza la VLAN nativa della porta trunk come configurata sullo switch.

Solo il traffico admin in entrata, ad esempio utilizzato per il traffico SSH, Grid Manager o Tenant Manager, è supportato sulle reti VLAN. Il traffico in uscita, ad esempio utilizzato per NTP, DNS, LDAP, KMS e Cloud Storage Pool, non è supportato sulle reti VLAN.



Le interfacce VLAN possono essere aggiunte solo ai nodi Admin e ai nodi Gateway. Non è possibile utilizzare un'interfaccia VLAN per l'accesso client o amministrativo ai nodi di storage o ai nodi di archivio.

Vedere [Configurare le interfacce VLAN](#) per istruzioni e linee guida.

Le interfacce VLAN vengono utilizzate solo nei gruppi ha e vengono assegnati indirizzi VIP sul nodo attivo. Vedere [Gestire i gruppi ad alta disponibilità](#) per istruzioni e linee guida.

Informazioni correlate

- [Requisiti di rete](#)

Esempi di topologia di rete

Topologia Grid Network

La topologia di rete più semplice viene creata configurando solo Grid Network.

Quando si configura Grid Network, si stabiliscono l'indirizzo IP host, la subnet mask e l'indirizzo IP gateway per l'interfaccia eth0 per ciascun nodo della griglia.

Durante la configurazione, è necessario aggiungere tutte le subnet Grid Network all'elenco di subnet Grid Network (GNSL). Questo elenco include tutte le subnet per tutti i siti e potrebbe includere anche sottoreti esterne che forniscono l'accesso a servizi critici come NTP, DNS o LDAP.

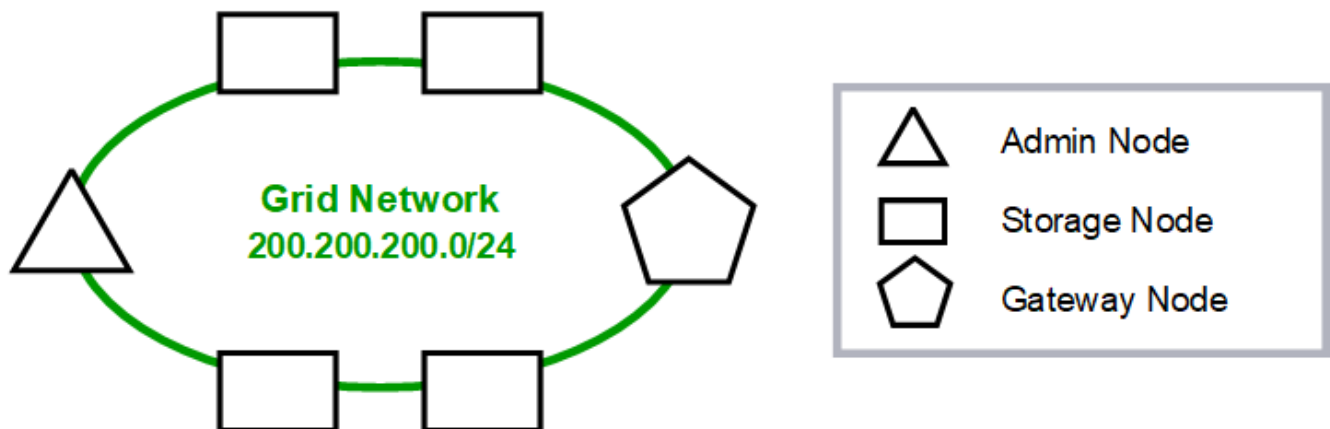
Al momento dell'installazione, l'interfaccia Grid Network applica route statiche per tutte le subnet in GNSL e imposta il percorso predefinito del nodo al gateway Grid Network, se configurato. GNSL non è richiesto se non esiste una rete client e il gateway Grid Network è il percorso predefinito del nodo. Vengono generati anche i percorsi host verso tutti gli altri nodi della griglia.

In questo esempio, tutto il traffico condivide la stessa rete, incluso il traffico relativo alle richieste dei client S3 e Swift e alle funzioni amministrative e di manutenzione.



Questa topologia è appropriata per implementazioni a singolo sito che non sono disponibili esternamente, implementazioni proof-of-concept o di test o quando un bilanciamento del carico di terze parti agisce come limite di accesso al client. Se possibile, la rete Grid deve essere utilizzata esclusivamente per il traffico interno. Sia la rete di amministrazione che la rete client presentano ulteriori restrizioni firewall che bloccano il traffico esterno verso i servizi interni. È supportato l'utilizzo di Grid Network per il traffico client esterno, ma questo tipo di utilizzo offre meno livelli di protezione.

Topology example: Grid Network only



GNSL → 200.200.200.0/24

Grid Network		
Nodes	IP/mask	Gateway
Admin	200.200.200.32/24	200.200.200.1
Storage	200.200.200.33/24	200.200.200.1
Storage	200.200.200.34/24	200.200.200.1
Storage	200.200.200.35/24	200.200.200.1
Storage	200.200.200.36/24	200.200.200.1
Gateway	200.200.200.37/24	200.200.200.1

System Generated

Nodes	Routes	Type	From
All	0.0.0.0/0 → 200.200.200.1	Default	Grid Network gateway
	200.200.200.0/24 → eth0	Link	Interface IP/mask

Topologia della rete amministrativa

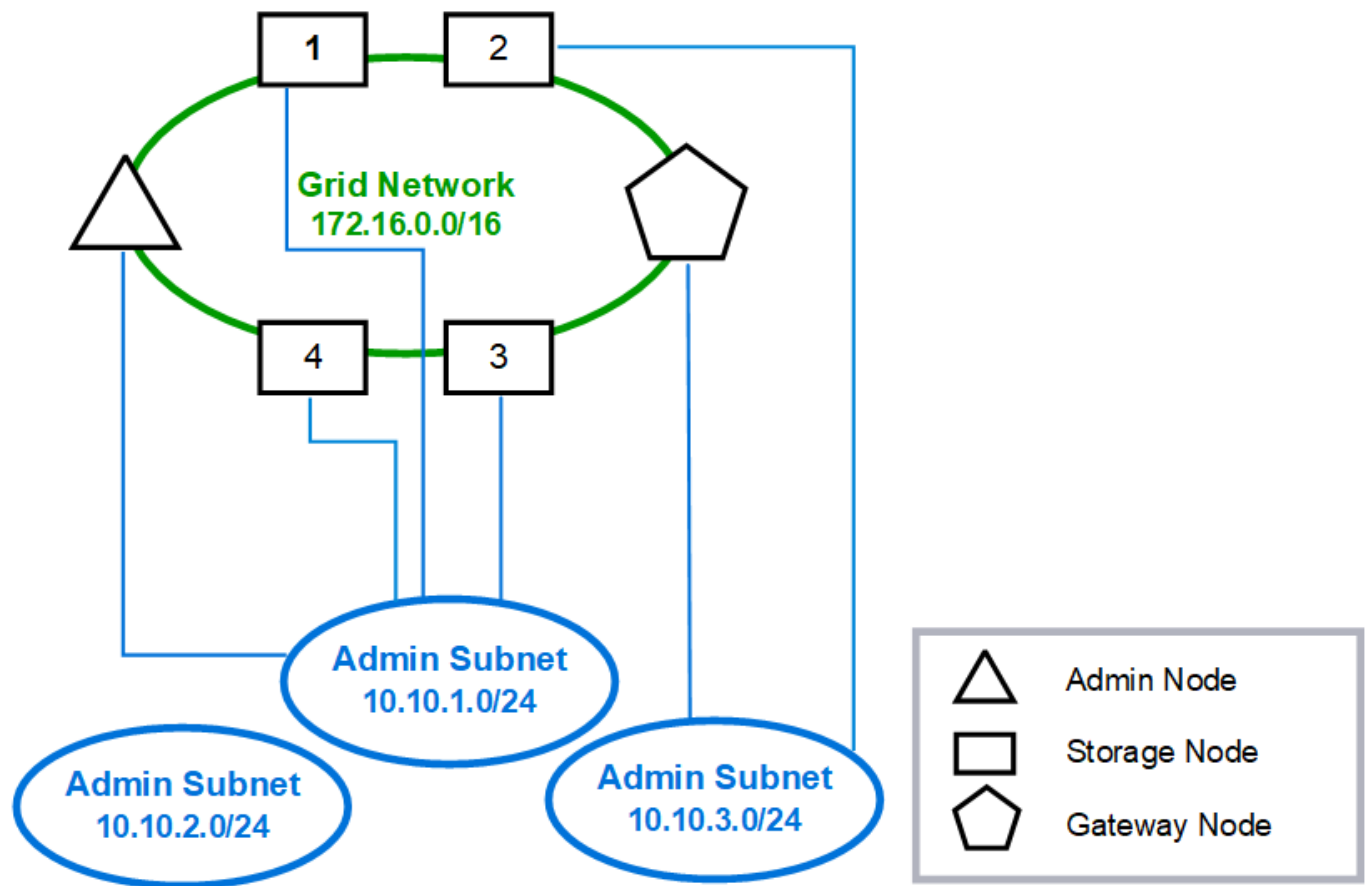
Disporre di una rete amministrativa è facoltativo. Un modo per utilizzare una rete amministrativa e una rete griglia consiste nel configurare una rete griglia inostradabile e una rete amministrativa limitata per ciascun nodo.

Quando si configura la rete amministrativa, si stabiliscono l'indirizzo IP host, la subnet mask e l'indirizzo IP gateway per l'interfaccia eth1 per ciascun nodo della griglia.

La rete amministrativa può essere univoca per ciascun nodo e può essere costituita da più sottoreti. Ciascun nodo può essere configurato con un Admin External Subnet List (AESL). AESL elenca le subnet raggiungibili tramite la rete di amministrazione per ciascun nodo. L'AESL deve includere anche le subnet di tutti i servizi a cui la griglia accede tramite la rete di amministrazione, come NTP, DNS, KMS e LDAP. Le route statiche vengono applicate a ciascuna subnet di AESL.

In questo esempio, Grid Network viene utilizzato per il traffico correlato alle richieste dei client S3 e Swift e alla gestione degli oggetti. Mentre la rete amministrativa viene utilizzata per le funzioni amministrative.

Topology example: Grid and Admin Networks



GNSL → 172.16.0.0/16

AESL (all) → 10.10.1.0/24 10.10.2.0/24 10.10.3.0/24

Nodes	Grid Network		Admin Network	
	IP/mask	Gateway	IP/mask	Gateway
Admin	172.16.200.32/24	172.16.200.1	10.10.1.10/24	10.10.1.1
Storage 1	172.16.200.33/24	172.16.200.1	10.10.1.11/24	10.10.1.1
Storage 2	172.16.200.34/24	172.16.200.1	10.10.3.65/24	10.10.3.1
Storage 3	172.16.200.35/24	172.16.200.1	10.10.1.12/24	10.10.1.1
Storage 4	172.16.200.36/24	172.16.200.1	10.10.1.13/24	10.10.1.1
Gateway	172.16.200.37/24	172.16.200.1	10.10.3.66/24	10.10.3.1

System Generated					
Nodes	Routes			Type	From
All	0.0.0.0/0	→	172.16.200.1	Default	Grid Network gateway
Admin, Storage 1, 3, and 4	172.16.0.0/16	→	eth0	Static	GNSL
	10.10.1.0/24	→	eth1	Link	Interface IP/mask
	10.10.2.0/24	→	10.10.1.1	Static	AESL
	10.10.3.0/24	→	10.10.1.1	Static	AESL
Storage 2, Gateway	172.16.0.0/16	→	eth0	Static	GNSL
	10.10.1.0/24	→	10.10.3.1	Static	AESL
	10.10.2.0/24	→	10.10.3.1	Static	AESL
	10.10.3.0/24	→	eth1	Link	Interface IP/mask

Topologia di rete del client

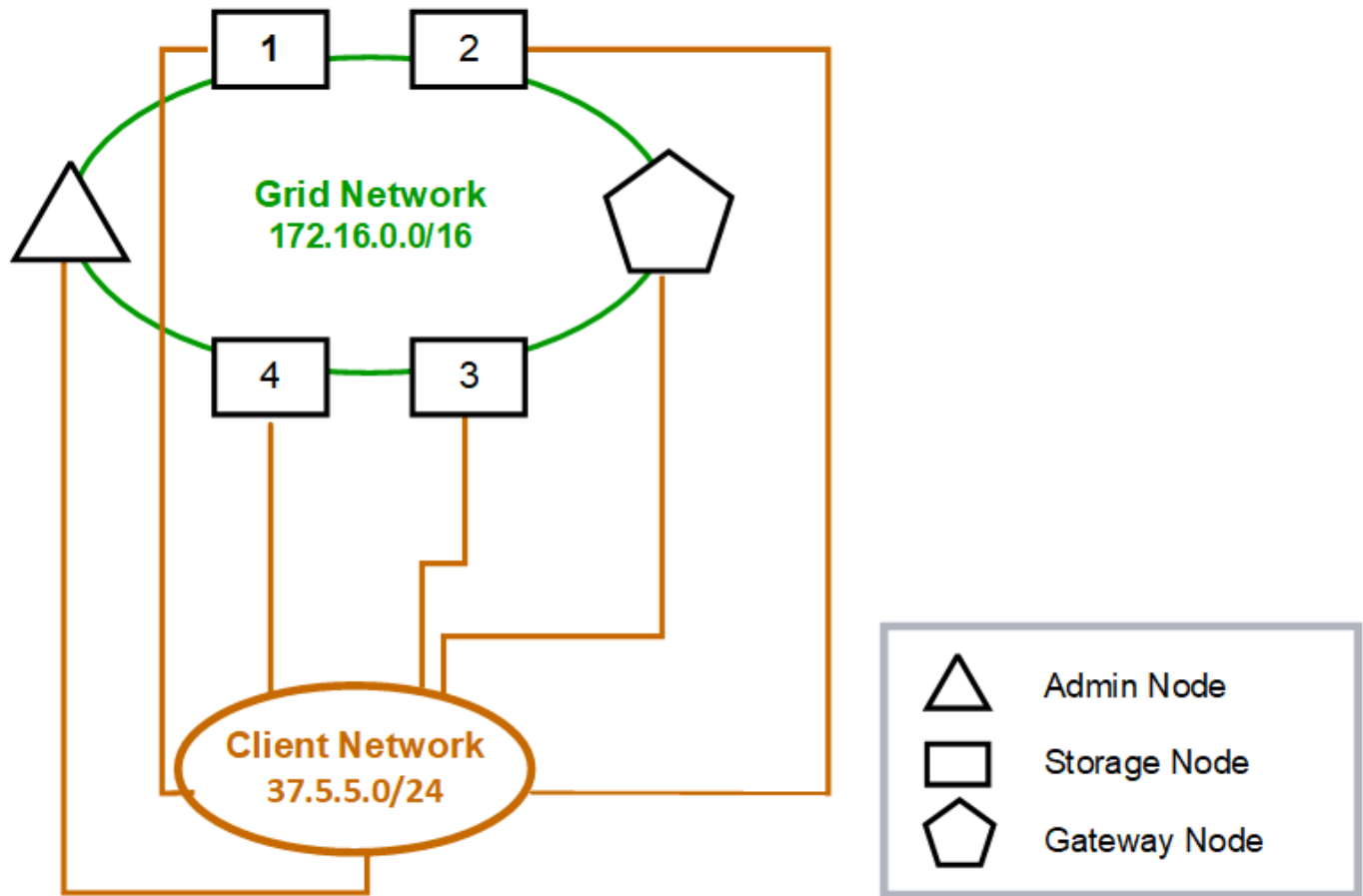
La disponibilità di una rete client è opzionale. L'utilizzo di una rete client consente di separare il traffico di rete client (ad esempio S3 e Swift) dal traffico interno della rete, consentendo una maggiore sicurezza delle reti di rete. Il traffico amministrativo può essere gestito dal client o dalla rete griglia quando la rete amministrativa non è configurata.

Quando si configura la rete client, vengono impostati l'indirizzo IP host, la subnet mask e l'indirizzo IP gateway per l'interfaccia eth2 per il nodo configurato. La rete client di ciascun nodo può essere indipendente dalla rete client di qualsiasi altro nodo.

Se si configura una rete client per un nodo durante l'installazione, il gateway predefinito del nodo passa dal gateway Grid Network al gateway Client Network al termine dell'installazione. Se viene aggiunta una rete client in un secondo momento, il gateway predefinito del nodo cambia nello stesso modo.

In questo esempio, la rete client viene utilizzata per le richieste dei client S3 e Swift e per le funzioni amministrative, mentre la rete griglia è dedicata alle operazioni di gestione degli oggetti interne.

Topology example: Grid and Client Networks



GNSL → 172.16.0.0/16

Nodes	Grid Network	Client Network	
	IP/mask	IP/mask	Gateway
Admin	172.16.200.32/24	37.5.5.10/24	37.5.5.1
Storage	172.16.200.33/24	37.5.5.11/24	37.5.5.1
Storage	172.16.200.34/24	37.5.5.12/24	37.5.5.1
Storage	172.16.200.35/24	37.5.5.13/24	37.5.5.1
Storage	172.16.200.36/24	37.5.5.14/24	37.5.5.1
Gateway	172.16.200.37/24	37.5.5.15/24	37.5.5.1

System Generated

Nodes	Routes		Type	From
All	0.0.0.0/0	→ 37.5.5.1	Default	Client Network gateway
	172.16.0.0/16	→ eth0	Link	Interface IP/mask
	37.5.5.0/24	→ eth2	Link	Interface IP/mask

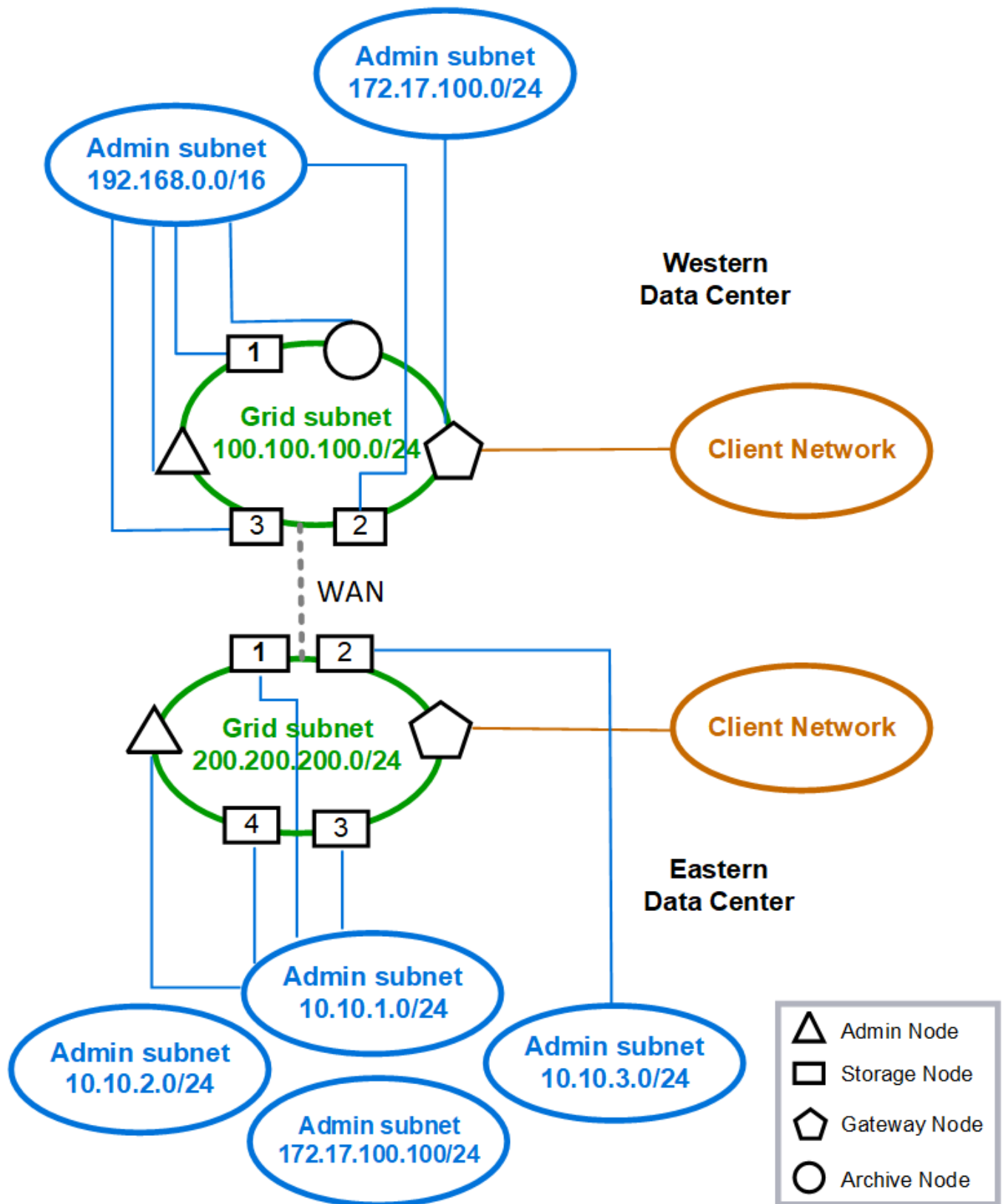
Topologia per tutte e tre le reti

È possibile configurare tutte e tre le reti in una topologia di rete costituita da una rete griglia privata, reti amministrative specifiche del sito delimitate e reti client aperte. L'utilizzo di endpoint di bilanciamento del carico e reti client non attendibili può fornire ulteriore sicurezza, se necessario.

In questo esempio:

- Grid Network viene utilizzato per il traffico di rete correlato alle operazioni di gestione degli oggetti interne.
- La rete amministrativa viene utilizzata per il traffico relativo alle funzioni amministrative.
- La rete client viene utilizzata per il traffico relativo alle richieste dei client S3 e Swift.

Topology example: Grid, Admin, and Client Networks



Requisiti di rete

È necessario verificare che l'infrastruttura e la configurazione di rete correnti siano in grado di supportare la progettazione pianificata della rete StorageGRID.

Requisiti generali di rete

Tutte le implementazioni StorageGRID devono essere in grado di supportare le seguenti connessioni.

Queste connessioni possono avvenire attraverso reti Grid, Admin o Client o le combinazioni di queste reti, come illustrato negli esempi di topologia di rete.

- **Connessioni di gestione:** Connessioni in entrata da un amministratore al nodo, in genere tramite SSH. Accesso del browser Web a Grid Manager, al tenant Manager e al programma di installazione dell'appliance StorageGRID.
- **Connessioni server NTP:** Connessione UDP in uscita che riceve una risposta UDP in entrata.

Almeno un server NTP deve essere raggiungibile dal nodo di amministrazione primario.

- **Connessioni server DNS:** Connessione UDP in uscita che riceve una risposta UDP in entrata.
- **Connessioni server LDAP/Active Directory:** Connessione TCP in uscita dal servizio identità sui nodi di storage.
- **AutoSupport:** Connessione TCP in uscita dai nodi di amministrazione a entrambi `support.netapp.com` o un proxy configurato dal cliente.
- **Server di gestione delle chiavi esterno:** Connessione TCP in uscita da ciascun nodo dell'appliance con crittografia del nodo attivata.
- Connessioni TCP in entrata da client S3 e Swift.
- Richieste in uscita dai servizi della piattaforma StorageGRID, come la replica di CloudMirror o dai pool di storage cloud.

Se StorageGRID non riesce a stabilire contatti con uno dei server NTP o DNS forniti utilizzando le regole di routing predefinite, tenterà automaticamente di contattare tutte le reti (griglia, amministratore e client), purché siano specificati gli indirizzi IP dei server DNS e NTP. Se i server NTP o DNS possono essere raggiunti su qualsiasi rete, StorageGRID crea automaticamente regole di routing aggiuntive per garantire che la rete venga utilizzata per tutti i tentativi futuri di connessione ad essa.



Sebbene sia possibile utilizzare questi percorsi host rilevati automaticamente, in generale è necessario configurare manualmente i percorsi DNS e NTP per garantire la connettività in caso di esito negativo del rilevamento automatico.

Se non si è pronti a configurare le reti opzionali Admin e Client durante l'implementazione, è possibile configurare queste reti quando si approvano i nodi Grid durante le fasi di configurazione. Inoltre, è possibile configurare queste reti dopo l'installazione, utilizzando lo strumento Change IP (vedere [Configurare gli indirizzi IP](#)).

Solo le connessioni client S3 e Swift e le connessioni amministrative SSH, Grid Manager e Tenant Manager sono supportate sulle interfacce VLAN. Connessioni in uscita, ad esempio a server NTP, DNS, LDAP, AutoSupport e KMS, Deve passare direttamente alle interfacce Client, Admin o Grid Network. Se l'interfaccia è configurata come trunk per supportare le interfacce VLAN, il traffico passa attraverso la VLAN nativa dell'interfaccia, come configurato sullo switch.

WAN (Wide Area Network) per più siti

Quando si configura un sistema StorageGRID con più siti, la connessione WAN tra siti deve avere una larghezza di banda minima di 25 Mbit/secondo in ciascuna direzione prima di tenere conto del traffico client. La replica dei dati o l'erasure coding tra siti, l'espansione di nodi o siti, il ripristino di nodi e altre operazioni o configurazioni richiedono una larghezza di banda aggiuntiva.

Connessioni per nodi Admin e nodi Gateway

I nodi di amministrazione devono essere sempre protetti da client non attendibili, ad esempio quelli su Internet aperto. È necessario assicurarsi che nessun client non attendibile possa accedere a qualsiasi nodo di amministrazione sulla rete griglia, sulla rete di amministrazione o sulla rete client.

I nodi di amministrazione e i nodi gateway che si intende aggiungere ai gruppi ad alta disponibilità devono essere configurati con un indirizzo IP statico. Per ulteriori informazioni, vedere [Gestire i gruppi ad alta disponibilità](#).

Utilizzo della NAT (Network Address Translation)

Non utilizzare NAT (Network Address Translation) sulla rete di rete tra nodi di rete o tra siti StorageGRID. Quando si utilizzano indirizzi IPv4 privati per Grid Network, tali indirizzi devono essere direttamente instradabili da ogni nodo di griglia in ogni sito. Tuttavia, se necessario, è possibile utilizzare NAT tra client esterni e nodi di rete, ad esempio per fornire un indirizzo IP pubblico per un nodo gateway. L'utilizzo di NAT per il bridge di un segmento di rete pubblica è supportato solo quando si utilizza un'applicazione di tunneling trasparente per tutti i nodi della griglia, il che significa che i nodi della griglia non richiedono alcuna conoscenza degli indirizzi IP pubblici.

Requisiti specifici della rete

Attenersi ai requisiti per ciascun tipo di rete StorageGRID.

Gateway e router di rete

- Se impostato, il gateway per una determinata rete deve trovarsi all'interno della subnet della rete specifica.
- Se si configura un'interfaccia utilizzando l'indirizzamento statico, è necessario specificare un indirizzo del gateway diverso da 0.0.0.0.
- Se non si dispone di un gateway, la procedura consigliata consiste nell'impostare l'indirizzo del gateway come indirizzo IP dell'interfaccia di rete.

Subnet



Ogni rete deve essere connessa alla propria sottorete che non si sovrappone ad altre reti del nodo.

Le seguenti restrizioni vengono applicate da Grid Manager durante l'implementazione. Vengono forniti qui per fornire assistenza nella pianificazione di rete pre-implementazione.

- La subnet mask per qualsiasi indirizzo IP di rete non può essere 255.255.255.254 o 255.255.255.255 (/31 o /32 nella notazione CIDR).
- La subnet definita da un indirizzo IP dell'interfaccia di rete e dalla subnet mask (CIDR) non può sovrapporsi alla subnet di qualsiasi altra interfaccia configurata sullo stesso nodo.
- La subnet Grid Network per ciascun nodo deve essere inclusa in GNSL.

- La subnet Admin Network non può sovrapporsi alla subnet Grid Network, alla subnet Client Network o a qualsiasi subnet in GNSL.
- Le subnet di AESL non possono sovrapporsi alle subnet di GNSL.
- La subnet della rete client non può sovrapporsi alla subnet della rete griglia, alla subnet della rete amministrativa, a qualsiasi subnet del GNSL o a qualsiasi subnet del sistema AESL.

Grid Network

- Al momento dell'implementazione, ciascun nodo della griglia deve essere collegato alla rete griglia e deve essere in grado di comunicare con l'Admin Node primario utilizzando la configurazione di rete specificata durante l'implementazione del nodo.
- Durante le normali operazioni di grid, ciascun nodo di grid deve essere in grado di comunicare con tutti gli altri nodi di grid sulla rete Grid.



La Grid Network deve essere instradabile direttamente tra ciascun nodo. NAT (Network Address Translation) tra nodi non supportato.

- Se la rete Grid è costituita da più sottoreti, aggiungerle all'elenco di subnet di rete Grid (GNSL). Le route statiche vengono create su tutti i nodi per ogni subnet nel GNSL.
- Se l'interfaccia Grid Network è configurata come trunk per supportare le interfacce VLAN, la VLAN nativa del trunk deve essere la VLAN utilizzata per il traffico Grid Network. Tutti i nodi della griglia devono essere accessibili tramite la VLAN nativa del trunk.

Admin Network (rete amministrativa)

La rete di amministrazione è opzionale. Se si intende configurare una rete amministrativa, attenersi ai seguenti requisiti e linee guida.

Gli utilizzi tipici della rete di amministrazione includono connessioni di gestione, AutoSupport, KMS e connessioni a server critici come NTP, DNS e LDAP, se queste connessioni non sono fornite attraverso la rete di rete o la rete client.



Admin Network e AESL possono essere univoci per ciascun nodo, purché i servizi di rete e i client desiderati siano raggiungibili.



Per abilitare le connessioni in entrata da sottoreti esterne, è necessario definire almeno una subnet sulla rete amministrativa. Le route statiche vengono generate automaticamente su ciascun nodo per ciascuna subnet dell'AESL.

Rete client

La rete client è opzionale. Se si intende configurare una rete client, tenere presente quanto segue.

- La rete client è progettata per supportare il traffico dai client S3 e Swift. Se configurato, il gateway di rete client diventa il gateway predefinito del nodo.
- Se si utilizza una rete client, è possibile proteggere StorageGRID da attacchi ostili accettando il traffico client in entrata solo su endpoint del bilanciamento del carico configurati esplicitamente. Vedere [Configurare gli endpoint del bilanciamento del carico](#).
- Se l'interfaccia di rete client è configurata come trunk per supportare le interfacce VLAN, valutare se è necessario configurare l'interfaccia di rete client (eth2). Se configurato, il traffico di rete client passa sulla

VLAN nativa del trunk, come configurato nello switch.

Considerazioni di rete specifiche per l'implementazione

Implementazioni Linux

Per garantire efficienza, affidabilità e sicurezza, il sistema StorageGRID viene eseguito su Linux come insieme di motori per container. La configurazione di rete relativa al motore dei container non è richiesta in un sistema StorageGRID.

Utilizzare un dispositivo non-bond, ad esempio una coppia VLAN o Virtual Ethernet (veth), per l'interfaccia di rete del container. Specificare questo dispositivo come interfaccia di rete nel file di configurazione del nodo.



Non utilizzare dispositivi bond o bridge direttamente come interfaccia di rete del container. In questo modo si potrebbe impedire l'avvio del nodo a causa di un problema del kernel con l'utilizzo di macvlan con dispositivi bond e bridge nello spazio dei nomi dei container.

Consultare le istruzioni di installazione per [Red Hat Enterprise Linux o CentOS](#) oppure [Ubuntu o Debian](#) implementazioni.

Configurazione della rete host per implementazioni di motori container

Prima di iniziare la distribuzione di StorageGRID su una piattaforma di motore container, determinare quali reti (griglia, amministratore, client) utilizzare ciascun nodo. È necessario assicurarsi che l'interfaccia di rete di ciascun nodo sia configurata sulla corretta interfaccia host virtuale o fisica e che ciascuna rete disponga di una larghezza di banda sufficiente.

Host fisici

Se si utilizzano host fisici per supportare i nodi grid:

- Assicurarsi che tutti gli host utilizzino la stessa interfaccia host per ogni interfaccia di nodo. Questa strategia semplifica la configurazione degli host e consente la migrazione futura dei nodi.
- Ottenere un indirizzo IP per l'host fisico stesso.



L'host può utilizzare un'interfaccia fisica sull'host e uno o più nodi in esecuzione sull'host. Gli indirizzi IP assegnati all'host o ai nodi che utilizzano questa interfaccia devono essere univoci. L'host e il nodo non possono condividere gli indirizzi IP.

- Aprire le porte necessarie per l'host.
- Se si intende utilizzare le interfacce VLAN in StorageGRID, l'host deve disporre di una o più interfacce di trunk che forniscono l'accesso alle VLAN desiderate. Queste interfacce possono essere passate nel contenitore di nodi come eth0, eth2 o come interfacce aggiuntive. Per aggiungere trunk o interfacce di accesso, vedere quanto segue:
 - **RHEL o CentOS (prima di installare il nodo):** [Creare file di configurazione del nodo](#)
 - **Ubuntu o Debian (prima di installare il nodo):** [Creare file di configurazione del nodo](#)
 - **RHEL, CentOS, Ubuntu o Debian (dopo aver installato il nodo):** [Linux: Aggiunta di interfacce di accesso o trunk a un nodo](#)

Consigli sulla larghezza di banda minima

La seguente tabella fornisce le raccomandazioni relative alla larghezza di banda minima per ciascun tipo di nodo StorageGRID e per ciascun tipo di rete. È necessario fornire a ciascun host fisico o virtuale una larghezza di banda di rete sufficiente per soddisfare i requisiti di larghezza di banda minima aggregata per il numero totale e il tipo di nodi StorageGRID che si intende eseguire su tale host.

Tipo di nodo	Tipo di rete		
	Griglia	Amministratore	Client
Amministratore	10 Gbps	1 Gbps	1 Gbps
Gateway	10 Gbps	1 Gbps	10 Gbps
Storage	10 Gbps	1 Gbps	10 Gbps
Archiviare	10 Gbps	1 Gbps	10 Gbps



Questa tabella non include la larghezza di banda DELLA SAN, necessaria per l'accesso allo storage condiviso. Se si utilizza uno storage condiviso a cui si accede tramite Ethernet (iSCSI o FCoE), è necessario eseguire il provisioning di interfacce fisiche separate su ciascun host per fornire una larghezza di banda SAN sufficiente. Per evitare di introdurre un collo di bottiglia, la larghezza di banda DELLA SAN per un determinato host deve corrispondere approssimativamente alla larghezza di banda aggregata della rete del nodo di storage per tutti i nodi di storage in esecuzione su quell'host.

Utilizzare la tabella per determinare il numero minimo di interfacce di rete da eseguire su ciascun host, in base al numero e al tipo di nodi StorageGRID che si intende eseguire su tale host.

Ad esempio, per eseguire un nodo Admin, un nodo Gateway e un nodo Storage su un singolo host:

- Connessione delle reti Grid e Admin sul nodo Admin (richiede $10 + 1 = 11$ Gbps)
- Connessione delle reti Grid e Client sul nodo gateway (richiede $10 + 10 = 20$ Gbps)
- Connessione della rete Grid sul nodo di storage (richiede 10 Gbps)

In questo scenario, è necessario fornire un minimo di $11 + 20 + 10 = 41$ Gbps di larghezza di banda di rete, che potrebbero essere soddisfatte da due interfacce da 40 Gbps o cinque interfacce da 10 Gbps, potenzialmente aggregate in linee e quindi condivise dalle tre o più VLAN che trasportano le subnet Grid, Admin e Client locali al data center fisico contenente l'host.

Per alcuni metodi consigliati per configurare le risorse fisiche e di rete sugli host del cluster StorageGRID in modo da prepararsi alla distribuzione di StorageGRID, consultare quanto segue:

- [Configurare la rete host \(Red Hat Enterprise Linux o CentOS\)](#)
- [Configurare la rete host \(Ubuntu o Debian\)](#)

Networking e porte per servizi di piattaforma e Cloud Storage Pool

Se si prevede di utilizzare i servizi della piattaforma StorageGRID o i pool di storage

cloud, è necessario configurare il grid networking e i firewall per garantire che gli endpoint di destinazione possano essere raggiunti.

Networking per servizi di piattaforma

Come descritto in [Gestire i servizi della piattaforma per i tenant](#) e [Cosa sono i servizi della piattaforma](#), i servizi della piattaforma includono servizi esterni che forniscono integrazione della ricerca, notifica degli eventi e replica di CloudMirror.

I servizi della piattaforma richiedono l'accesso dai nodi di storage che ospitano il servizio ADC StorageGRID agli endpoint del servizio esterno. Esempi per fornire l'accesso includono:

- Sui nodi di storage con servizi ADC, configurare reti amministrative univoche con voci AESL che instradano verso gli endpoint di destinazione.
- Fare affidamento sul percorso predefinito fornito da una rete client. Se si utilizza il percorso predefinito, è possibile utilizzare [Funzione Untrusted Client Network](#) per limitare le connessioni in entrata.

Networking per i Cloud Storage Pools

I pool di cloud storage richiedono inoltre l'accesso dai nodi di storage agli endpoint forniti dal servizio esterno utilizzato, come Amazon S3 Glacier o Microsoft Azure Blob. Per ulteriori informazioni, vedere [Cos'è un pool di storage cloud](#).

Porte per servizi di piattaforma e Cloud Storage Pools

Per impostazione predefinita, i servizi della piattaforma e le comunicazioni del Cloud Storage Pool utilizzano le seguenti porte:

- **80:** Per gli URI endpoint che iniziano con `http`
- **443:** Per gli URI endpoint che iniziano con `https`

È possibile specificare una porta diversa quando si crea o si modifica l'endpoint. Vedere [Riferimento porta di rete](#).

Se si utilizza un server proxy non trasparente, è necessario anche [configurare le impostazioni del proxy di storage](#) per consentire l'invio dei messaggi a endpoint esterni, ad esempio un endpoint su internet.

VLAN, servizi di piattaforma e Cloud Storage Pool

Non è possibile utilizzare reti VLAN per servizi di piattaforma o Cloud Storage Pool. Gli endpoint di destinazione devono essere raggiungibili tramite la rete Grid, Admin o Client.

Nodi appliance

È possibile configurare le porte di rete sulle appliance StorageGRID in modo che utilizzino le modalità di port bond che soddisfano i requisiti di throughput, ridondanza e failover.

Le porte 10/25-GbE delle appliance StorageGRID possono essere configurate in modalità bond fissa o aggregata per le connessioni alla rete grid e alla rete client.

Le porte di Admin Network 1-GbE possono essere configurate in modalità indipendente o Active-Backup per le connessioni alla rete di amministrazione.

Consultare le informazioni relative alle modalità di port bond nelle istruzioni di installazione e manutenzione dell'appliance:

- [Appliance di servizi SG100 e SG1000](#)
- [Appliance di storage SG6000](#)
- [Appliance di storage SG5700](#)
- [Appliance di storage SG5600](#)

Installazione e provisioning di rete

È necessario comprendere in che modo la rete grid e le reti amministrative e client opzionali vengono utilizzate durante l'implementazione del nodo e la configurazione del grid.

Implementazione iniziale di un nodo

Quando si implementa per la prima volta un nodo, è necessario collegarlo alla rete Grid e assicurarsi che disponga dell'accesso al nodo Admin primario. Se la rete Grid è isolata, è possibile configurare la rete Admin sul nodo Admin primario per l'accesso alla configurazione e all'installazione dall'esterno della rete Grid.

Una rete Grid con un gateway configurato diventa il gateway predefinito per un nodo durante l'implementazione. Il gateway predefinito consente ai nodi della griglia su sottoreti separate di comunicare con il nodo di amministrazione primario prima che la griglia sia stata configurata.

Se necessario, le subnet contenenti server NTP o che richiedono l'accesso a Grid Manager o API possono anche essere configurate come subnet della griglia.

Registrazione automatica del nodo con nodo di amministrazione primario

Una volta implementati, i nodi si registrano con il nodo di amministrazione primario utilizzando la rete di griglia. È quindi possibile utilizzare Grid Manager, il `configure-storagegrid.py` Python o l'API di installazione per configurare la griglia e approvare i nodi registrati. Durante la configurazione della griglia, è possibile configurare più subnet della griglia. I percorsi statici a queste subnet attraverso il gateway Grid Network verranno creati su ciascun nodo al termine della configurazione della griglia.

Disattivazione della rete amministrativa o della rete client

Se si desidera disattivare Admin Network o Client Network, è possibile rimuovere la configurazione durante il processo di approvazione del nodo oppure utilizzare lo strumento Change IP una volta completata l'installazione (vedere [Configurare gli indirizzi IP](#)).

Linee guida per la post-installazione

Dopo aver completato l'implementazione e la configurazione del nodo griglia, seguire queste linee guida per l'indirizzamento DHCP e le modifiche alla configurazione di rete.

- Se si utilizza DHCP per assegnare indirizzi IP, configurare una prenotazione DHCP per ciascun indirizzo IP sulle reti utilizzate.

È possibile configurare DHCP solo durante la fase di implementazione. Non è possibile impostare DHCP durante la configurazione.



I nodi si riavviano quando cambiano gli indirizzi IP, causando interruzioni se una modifica dell'indirizzo DHCP influisce su più nodi contemporaneamente.

- Per modificare gli indirizzi IP, le subnet mask e i gateway predefiniti di un nodo griglia, è necessario utilizzare le procedure Change IP (Modifica IP). Vedere [Configurare gli indirizzi IP](#).
- Se si apportano modifiche alla configurazione di rete, incluse modifiche al routing e al gateway, la connettività del client al nodo di amministrazione primario e ad altri nodi della griglia potrebbe andare persa. A seconda delle modifiche di rete applicate, potrebbe essere necessario ristabilire queste connessioni.

Riferimento porta di rete

È necessario garantire che l'infrastruttura di rete possa fornire comunicazioni interne ed esterne tra i nodi all'interno della griglia e a client e servizi esterni. Potrebbe essere necessario accedere a firewall interni ed esterni, sistemi di switching e sistemi di routing.

Utilizzare i dettagli forniti per [Comunicazioni interne al nodo di rete](#) e [Comunicazioni esterne](#) per determinare come configurare ciascuna porta richiesta.

Comunicazioni interne al nodo di rete

Il firewall interno di StorageGRID consente solo connessioni in entrata a porte specifiche della rete di rete, ad eccezione delle porte 22, 80, 123 e 443 (vedere le informazioni sulle comunicazioni esterne). Le connessioni sono accettate anche sulle porte definite dagli endpoint del bilanciamento del carico.



NetApp consiglia di attivare il traffico ICMP (Internet Control message Protocol) tra i nodi di rete. Consentire il traffico ICMP può migliorare le prestazioni di failover quando non è possibile raggiungere un nodo di rete.

Oltre a ICMP e alle porte elencate nella tabella, StorageGRID utilizza il protocollo di ridondanza del router virtuale (VRRP). VRRP è un protocollo Internet che utilizza il protocollo IP numero 112. StorageGRID utilizza VRRP solo in modalità unicast. VRRP è richiesto solo se [gruppi ad alta disponibilità](#) sono configurati.

Linee guida per i nodi basati su Linux

Se i criteri di rete aziendali limitano l'accesso a una di queste porte, è possibile rimappare le porte in fase di implementazione utilizzando un parametro di configurazione dell'implementazione. Per ulteriori informazioni sul remapping delle porte e sui parametri di configurazione della distribuzione, vedere:

- [Installare Red Hat Enterprise Linux o CentOS](#)
- [Installare Ubuntu o Debian](#)

Linee guida per i nodi basati su VMware

Configurare le seguenti porte solo se è necessario definire restrizioni firewall esterne alla rete VMware.

Se i criteri di rete aziendali limitano l'accesso a una qualsiasi di queste porte, è possibile rimappare le porte quando si implementano nodi utilizzando VMware vSphere Web Client o utilizzando un'impostazione del file di configurazione quando si automatizza l'implementazione del nodo grid. Per ulteriori informazioni sul remapping delle porte e sui parametri di configurazione della distribuzione, vedere [Installare VMware](#).

Linee guida per i nodi appliance

Se i criteri di rete aziendali limitano l'accesso a una di queste porte, è possibile rimappare le porte utilizzando il programma di installazione dell'appliance StorageGRID. Per ulteriori informazioni sul rimapping delle porte per le appliance, consulta:

- [Appliance di servizi SG100 e SG1000](#)
- [Appliance di storage SG6000](#)
- [Appliance di storage SG5700](#)
- [Appliance di storage SG5600](#)

Porte interne StorageGRID

Porta	TCP o UDP	Da	A.	Dettagli
22	TCP	Nodo amministratore primario	Tutti i nodi	Per le procedure di manutenzione, il nodo di amministrazione primario deve essere in grado di comunicare con tutti gli altri nodi utilizzando SSH sulla porta 22. Consentire il traffico SSH da altri nodi è facoltativo.
80	TCP	Appliance	Nodo amministratore primario	Utilizzato dalle appliance StorageGRID per comunicare con il nodo di amministrazione principale per avviare l'installazione.
123	UDP	Tutti i nodi	Tutti i nodi	Servizio Network Time Protocol. Ogni nodo sincronizza il proprio tempo con ogni altro nodo utilizzando NTP.

443	TCP	Tutti i nodi	Nodo amministratore primario	Utilizzato per comunicare lo stato al nodo di amministrazione primario durante l'installazione e altre procedure di manutenzione.
1139	TCP	Nodi di storage	Nodi di storage	Traffico interno tra nodi di storage.
1501	TCP	Tutti i nodi	Nodi di storage con ADC	Traffico interno di reporting, controllo e configurazione.
1502	TCP	Tutti i nodi	Nodi di storage	Traffico interno correlato a S3 e Swift.
1504	TCP	Tutti i nodi	Nodi di amministrazione	Traffico interno di configurazione e reporting del servizio NMS.
1505	TCP	Tutti i nodi	Nodi di amministrazione	Traffico interno del servizio AMS.
1506	TCP	Tutti i nodi	Tutti i nodi	Traffico interno dello stato del server.
1507	TCP	Tutti i nodi	Nodi gateway	Traffico interno del bilanciamento del carico.
1508	TCP	Tutti i nodi	Nodo amministratore primario	Traffico interno della gestione della configurazione.
1509	TCP	Tutti i nodi	Nodi di archiviazione	Traffico interno del nodo di archiviazione.
1511	TCP	Tutti i nodi	Nodi di storage	Traffico interno dei metadati.

5353	UDP	Tutti i nodi	Tutti i nodi	Utilizzato come opzione per le modifiche dell'IP full-grid e per il rilevamento del nodo di amministrazione primario durante l'installazione, l'espansione e il ripristino.
7001	TCP	Nodi di storage	Nodi di storage	Comunicazione cluster tra nodi Cassandra TLS.
7443	TCP	Tutti i nodi	Nodi di amministrazione	Traffico interno per le procedure di manutenzione e la segnalazione degli errori.
8443	TCP	Nodo amministratore primario	Nodi appliance	Traffico interno relativo alla procedura della modalità di manutenzione.
9042	TCP	Nodi di storage	Nodi di storage	Porta client Cassandra.
9999	TCP	Tutti i nodi	Tutti i nodi	Traffico interno per più servizi. Include procedure di manutenzione, metriche e aggiornamenti di rete.
10226	TCP	Nodi di storage	Nodo amministratore primario	Utilizzato dalle appliance StorageGRID per l'inoltro dei messaggi AutoSupport da Gestione di sistema di e-Series SANtricity al nodo di amministrazione primario.

11139	TCP	Nodi di archiviazione/storage e	Nodi di archiviazione/storage e	Traffico interno tra nodi di storage e nodi di archiviazione.
18000	TCP	Nodi Admin/Storage	Nodi di storage con ADC	Traffico interno del servizio account.
18001	TCP	Nodi Admin/Storage	Nodi di storage con ADC	Traffico interno di Identity Federation.
18002	TCP	Nodi Admin/Storage	Nodi di storage	Traffico API interno correlato ai protocolli a oggetti.
18003	TCP	Nodi Admin/Storage	Nodi di storage con ADC	Traffico interno dei servizi della piattaforma.
18017	TCP	Nodi Admin/Storage	Nodi di storage	Traffico interno del servizio Data Mover per i pool di storage cloud.
18019	TCP	Nodi di storage	Nodi di storage	Traffico interno del servizio di chunk per la cancellazione del codice.
18082	TCP	Nodi Admin/Storage	Nodi di storage	Traffico interno correlato a S3.
18083	TCP	Tutti i nodi	Nodi di storage	Traffico interno correlato a Swift.
18200	TCP	Nodi Admin/Storage	Nodi di storage	Statistiche aggiuntive sulle richieste dei client.
19000	TCP	Nodi Admin/Storage	Nodi di storage con ADC	Traffico interno del servizio Keystone.

Informazioni correlate

[Comunicazioni esterne](#)

Comunicazioni esterne

I client devono comunicare con i nodi grid per acquisire e recuperare contenuti. Le porte

utilizzate dipendono dai protocolli di storage a oggetti scelti. Queste porte devono essere accessibili al client.

Accesso limitato alle porte

Se i criteri di rete aziendali limitano l'accesso a una delle porte, è possibile utilizzare [endpoint del bilanciamento del carico](#) per consentire l'accesso alle porte definite dall'utente. È quindi possibile utilizzare [Reti client non attendibili](#) per consentire l'accesso solo sulle porte endpoint del bilanciamento del carico.

Rimappatura delle porte

Per utilizzare sistemi e protocolli come SMTP, DNS, SSH o DHCP, è necessario rimappare le porte durante l'implementazione dei nodi. Tuttavia, non è necessario rimappare gli endpoint del bilanciamento del carico. Per informazioni sul remapping delle porte, consultare le istruzioni di installazione della piattaforma:

Nodi basati su software

- [Installare Red Hat Enterprise Linux o CentOS](#)
- [Installare Ubuntu o Debian](#)
- [Installare VMware](#)

Nodi appliance

- [Appliance di servizi SG100 e SG1000](#)
- [Appliance di storage SG6000](#)
- [Appliance di storage SG5700](#)
- [Appliance di storage SG5600](#)

Porte utilizzate per le comunicazioni esterne

La seguente tabella mostra le porte utilizzate per il traffico nei nodi.



Questo elenco non include le porte che potrebbero essere configurate come [endpoint del bilanciamento del carico](#) o utilizzato per "server syslog".

Porta	TCP o UDP	Protocollo	Da	A.	Dettagli
22	TCP	SSH	Laptop di assistenza	Tutti i nodi	L'accesso a SSH o alla console è necessario per le procedure con le procedure della console. In alternativa, è possibile utilizzare la porta 2022 invece della porta 22.
25	TCP	SMTP	Nodi di amministrazione	Server di posta elettronica	Utilizzato per avvisi e AutoSupport basato su e-mail. È possibile ignorare l'impostazione predefinita della porta 25 utilizzando la pagina Server di posta elettronica.

Porta	TCP o UDP	Protocollo	Da	A.	Dettagli
53	TCP/UDP	DNS	Tutti i nodi	Server DNS	Utilizzato per il sistema dei nomi di dominio.
67	UDP	DHCP	Tutti i nodi	Servizio DHCP	Utilizzato come opzione per supportare la configurazione di rete basata su DHCP. Il servizio dhclient non viene eseguito per le griglie configurate staticamente.
68	UDP	DHCP	Servizio DHCP	Tutti i nodi	Utilizzato come opzione per supportare la configurazione di rete basata su DHCP. Il servizio dhclient non viene eseguito per le griglie che utilizzano indirizzi IP statici.
80	TCP	HTTP	Browser	Nodi di amministrazione	La porta 80 reindirizza alla porta 443 per l'interfaccia utente del nodo di amministrazione.
80	TCP	HTTP	Browser	Appliance	La porta 80 viene reindirizzata alla porta 8443 per il programma di installazione dell'appliance StorageGRID.
80	TCP	HTTP	Nodi di storage con ADC	AWS	Utilizzato per i messaggi dei servizi della piattaforma inviati ad AWS o ad altri servizi esterni che utilizzano HTTP. I tenant possono eseguire l'override dell'impostazione predefinita della porta HTTP di 80 quando creano un endpoint.
80	TCP	HTTP	Nodi di storage	AWS	Richieste di Cloud Storage Pools inviate a destinazioni AWS che utilizzano HTTP. Gli amministratori della griglia possono ignorare l'impostazione predefinita della porta HTTP di 80 quando configurano un Cloud Storage Pool.

Porta	TCP o UDP	Protocollo	Da	A.	Dettagli
111	TCP/UDP	Rpcbind	Client NFS	Nodi di amministrazione	Utilizzato dall'esportazione di audit basata su NFS (portmap). Nota: questa porta è necessaria solo se è abilitata l'esportazione di audit basata su NFS.
123	UDP	NTP	Nodi NTP primari	NTP esterno	Servizio Network Time Protocol. I nodi selezionati come origini NTP primarie sincronizzano anche gli orari con le origini temporali NTP esterne.
137	UDP	NetBIOS	Client SMB	Nodi di amministrazione	Utilizzato dall'esportazione di audit basata su SMB per i client che richiedono il supporto NetBIOS. Nota: questa porta è necessaria solo se è abilitata l'esportazione di audit basata su SMB.
138	UDP	NetBIOS	Client SMB	Nodi di amministrazione	Utilizzato dall'esportazione di audit basata su SMB per i client che richiedono il supporto NetBIOS. Nota: questa porta è necessaria solo se è abilitata l'esportazione di audit basata su SMB.
139	TCP	PMI	Client SMB	Nodi di amministrazione	Utilizzato dall'esportazione di audit basata su SMB per i client che richiedono il supporto NetBIOS. Nota: questa porta è necessaria solo se è abilitata l'esportazione di audit basata su SMB.

Porta	TCP o UDP	Protocollo	Da	A.	Dettagli
161	TCP/UDP	SNMP	Client SNMP	Tutti i nodi	<p>Utilizzato per il polling SNMP. Tutti i nodi forniscono informazioni di base; i nodi di amministrazione forniscono anche dati di allarme e allarme. Impostazione predefinita della porta UDP 161 quando configurata.</p> <p>Nota: questa porta è necessaria solo e viene aperta sul firewall del nodo solo se SNMP è configurato. Se si intende utilizzare SNMP, è possibile configurare porte alternative.</p> <p>Nota: per informazioni sull'utilizzo di SNMP con StorageGRID, contattare il proprio rappresentante NetApp.</p>
162	TCP/UDP	Notifiche SNMP	Tutti i nodi	Destinazioni di notifica	<p>Per impostazione predefinita, le notifiche e i trap SNMP in uscita sono impostati sulla porta UDP 162.</p> <p>Nota: questa porta è necessaria solo se SNMP è attivato e le destinazioni di notifica sono configurate. Se si intende utilizzare SNMP, è possibile configurare porte alternative.</p> <p>Nota: per informazioni sull'utilizzo di SNMP con StorageGRID, contattare il proprio rappresentante NetApp.</p>
389	TCP/UDP	LDAP	Nodi di storage con ADC	Active Directory/LDAP	Utilizzato per la connessione a un server Active Directory o LDAP per Identity Federation.
443	TCP	HTTPS	Browser	Nodi di amministrazione	Utilizzato dai browser Web e dai client API di gestione per accedere a Grid Manager e Tenant Manager.

Porta	TCP o UDP	Protocollo	Da	A.	Dettagli
443	TCP	HTTPS	Nodi di amministrazione	Active Directory	Utilizzato dai nodi amministrativi che si connettono ad Active Directory se è attivato il Single Sign-on (SSO).
443	TCP	HTTPS	Nodi di archiviazione	Amazon S3	Utilizzato per accedere ad Amazon S3 dai nodi di archiviazione.
443	TCP	HTTPS	Nodi di storage con ADC	AWS	Utilizzato per i messaggi dei servizi della piattaforma inviati ad AWS o ad altri servizi esterni che utilizzano HTTPS. I tenant possono eseguire l'override dell'impostazione predefinita della porta HTTP di 443 quando creano un endpoint.
443	TCP	HTTPS	Nodi di storage	AWS	Richieste di Cloud Storage Pools inviate a destinazioni AWS che utilizzano HTTPS. Gli amministratori della griglia possono ignorare l'impostazione predefinita della porta HTTPS 443 quando configurano un Cloud Storage Pool.
445	TCP	PMI	Client SMB	Nodi di amministrazione	Utilizzato dall'esportazione di audit basata su SMB. Nota: questa porta è necessaria solo se è abilitata l'esportazione di audit basata su SMB.
903	TCP	NFS	Client NFS	Nodi di amministrazione	Utilizzato dall'esportazione di audit basata su NFS (<code>rpc.mountd</code>). Nota: questa porta è necessaria solo se è abilitata l'esportazione di audit basata su NFS.

Porta	TCP o UDP	Protocollo	Da	A.	Dettagli
2022	TCP	SSH	Laptop di assistenza	Tutti i nodi	L'accesso a SSH o alla console è necessario per le procedure con le procedure della console. In alternativa, è possibile utilizzare la porta 22 invece della porta 2022.
2049	TCP	NFS	Client NFS	Nodi di amministrazione	Utilizzato da NFS (NFS-based audit export). Nota: questa porta è necessaria solo se è abilitata l'esportazione di audit basata su NFS.
5696	TCP	KMIP	Appliance	KM	Traffico esterno del protocollo KMIP (Key Management Interoperability Protocol) dalle appliance configurate per la crittografia del nodo al server di gestione delle chiavi (KMS), a meno che non sia specificata una porta diversa nella pagina di configurazione KMS del programma di installazione dell'appliance StorageGRID.
8022	TCP	SSH	Laptop di assistenza	Tutti i nodi	SSH sulla porta 8022 garantisce l'accesso al sistema operativo di base sulle piattaforme di appliance e nodi virtuali per il supporto e la risoluzione dei problemi. Questa porta non viene utilizzata per i nodi basati su Linux (bare metal) e non è necessaria per essere accessibile tra i nodi di rete o durante le normali operazioni.
8082	TCP	HTTPS	Client S3	Nodi gateway	Traffico del client S3 verso il servizio CLB obsoleto sui nodi gateway (HTTPS).
8083	TCP	HTTPS	Client Swift	Nodi gateway	Traffico client rapido verso il servizio CLB obsoleto sui nodi gateway (HTTPS).

Porta	TCP o UDP	Protocollo	Da	A.	Dettagli
8084	TCP	HTTP	Client S3	Nodi gateway	Traffico del client S3 verso il servizio CLB obsoleto sui nodi gateway (HTTP).
8085	TCP	HTTP	Client Swift	Nodi gateway	Traffico client rapido verso il servizio CLB obsoleto sui nodi gateway (HTTP).
8443	TCP	HTTPS	Browser	Nodi di amministrazione	Opzionale. Utilizzato dai browser Web e dai client API di gestione per l'accesso a Grid Manager. Può essere utilizzato per separare le comunicazioni di Grid Manager e Tenant Manager.
9022	TCP	SSH	Laptop di assistenza	Appliance	Concede l'accesso alle appliance StorageGRID in modalità pre-configurazione per il supporto e la risoluzione dei problemi. Non è necessario che questa porta sia accessibile tra i nodi della griglia o durante le normali operazioni.
9091	TCP	HTTPS	Servizio Grafana esterno	Nodi di amministrazione	Utilizzato dai servizi esterni Grafana per un accesso sicuro al servizio StorageGRID Prometheus. Nota: questa porta è necessaria solo se è abilitato l'accesso Prometheus basato su certificato.
9443	TCP	HTTPS	Browser	Nodi di amministrazione	Opzionale. Utilizzato dai browser Web e dai client API di gestione per l'accesso a Tenant Manager. Può essere utilizzato per separare le comunicazioni di Grid Manager e Tenant Manager.
18082	TCP	HTTPS	Client S3	Nodi di storage	Traffico del client S3 direttamente ai nodi di storage (HTTPS).

Porta	TCP o UDP	Protocollo	Da	A.	Dettagli
18083	TCP	HTTPS	Client Swift	Nodi di storage	Traffico client rapido direttamente ai nodi di storage (HTTPS).
18084	TCP	HTTP	Client S3	Nodi di storage	Traffico del client S3 direttamente ai nodi di storage (HTTP).
18085	TCP	HTTP	Client Swift	Nodi di storage	Traffico client rapido direttamente ai nodi di storage (HTTP).

Informazioni sul copyright

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

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

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

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

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

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

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

Informazioni sul marchio commerciale

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